VERITAS NetBackup 4.5 Shared Storage Option™

System Administrator's Guide

for UNIX and Windows

March 2002
30-000515-011

VERITAS

Disclaimer

The information contained in this publication is subject to change without notice. VERITAS Software Corporation makes no warranty of any kind with regard to this manual, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. VERITAS Software Corporation shall not be liable for errors contained herein or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual.

Copyright

VERITAS Software Corporation
350 Ellis Street
Mountain View, CA 94043
USA
Phone 650–527–8000
Fax 650-527-2908
www.veritas.com

Contents

About This Guide

Introduction

The Shared Storage Option (SSO) is available as a separately licensed and priced software option available only with VERITAS NetBackup DataCenter.

SSO runs on Windows and UNIX servers (see “Supported Servers” on page 88). This option requires appropriate hardware connectivity.

SSO is an extension to tape drive allocation and configuration for NetBackup Media Manager. Media Manager is the component of NetBackup DataCenter, VERITAS Storage Migrator, and VERITAS Storage Migrator Remote that manages devices and media.

Audience

The main audience for this guide is the system administrator responsible for installing SAN hardware, and installing and configuring SSO software.

This guide assumes a thorough knowledge of UNIX and Windows operating systems and hardware device configuration.

Scope

This version of this SSO guide

- Is intended for use only with the NetBackup DataCenter product for UNIX servers or Windows servers.

  SSO is not available with the NetBackup BusinesServer product.

- Is based on the capabilities and features of the 4.5 NetBackup DataCenter release.

  SSO-related differences between this release and the 3.4 NetBackup DataCenter release are noted in the NetBackup release notes.

- Contains many topics that refer to software and hardware configuration in general terms. In these topics, both Windows *and* UNIX servers are implied.

Some topics in this guide are specific to Windows servers or to specific Windows servers. Also some topics are specific to UNIX servers or to specific UNIX servers. The intended servers for these topics are noted in the text.

- Covers installation, configuration, and verification of SSO-related hardware in general terms. SSO runs with a multitude of hardware configurations; however, this guide provides only minimal configuration information for specific combinations of vendor hardware products, such as bridges and switches.

Organization

This guide contains the following chapters and an index, and is organized as follows:

Introduction to SSO

- "Introduction" on page 1 provides an overview of SSO and SAN. This chapter also includes a table of the steps you need to follow to install and use SSO, and their chapter locations in this guide.

Installation, Configuration, and Usage

- "Installing and Configuring Your SSO Hardware" on page 11 provides a general procedure to follow when configuring hardware for use with SSO.
- "Verifying Your SSO Hardware Is Connected and Working" on page 27 provides information on verifying your hardware configuration.
- "Installing the Shared Storage Option" on page 29 contains SSO software installation information.
- "Configuring SSO Devices and Media In Media Manager" on page 35 explains how to define your SSO configuration in Media Manager.
- "Verifying Your SSO Configuration" on page 53 provides information on verifying your Media Manager SSO configuration.
- "Configuring SSO Usage in NetBackup" on page 61 explains what needs to be done in the NetBackup storage unit and backup policy management interfaces to use SSO.
- "Using SSO" on page 65 explains how to obtain Media Manager SSO configuration information and fine tune SSO.

Advanced Topics

- "SCSI Reserve / Release" on page 71 provides information on the use of SCSI reserve / release commands by SSO to improve data integrity in an SSO configuration.

- "Troubleshooting Tips" on page 81 provides some ideas for troubleshooting SSO problems.
- "SSO Reference Topics" on page 87 contains important SSO reference topics.

Related Documents

NetBackup documents that may be useful are listed below. For a complete list of related documents, see the NetBackup release notes. Depending on your configuration, other documents may also be required.

- *NetBackup Release Notes for UNIX and Windows*

  Provides important information about NetBackup DataCenter and BusinesServer products on UNIX- and Windows-based servers, such as the platforms and operating systems that are supported and operating notes that may not be in the NetBackup manuals or the online help.

If your configuration includes UNIX servers, you may need the following manuals:

- *NetBackup Installation Guide for UNIX*

  Explains how to install NetBackup DataCenter software on UNIX-based platforms.

- *NetBackup DataCenter Media Manager System Administrator's Guide for UNIX*

  Explains how to configure and manage storage devices and media in Media Manager. Media Manager is part of the NetBackup DataCenter product.

- *NetBackup DataCenter System Administrator's Guide for UNIX*

  Explains how to configure and manage NetBackup DataCenter on a UNIX system.

- *NetBackup Media Manager Device Configuration Guide for UNIX*

  Explains how to add device drivers and perform other system-level configurations for storage devices that are supported by NetBackup DataCenter and NetBackup BusinesServer Media Manager on UNIX hosts.

- *NetBackup ServerFree Agent System Administrator's Guide for UNIX*

  Explains how to install, configure, and use ServerFree Agent for frozen image and SAN offhost backups.

- *NetBackup Troubleshooting Guide for UNIX*

  Provides troubleshooting information for UNIX-based NetBackup DataCenter and BusinesServer products.

- *VERITAS Storage Migrator Release Notes for UNIX*

Provides information such as the platforms and operating systems that are supported and operating notes that may not be in the Storage Migrator manuals.

- *VERITAS Storage Migrator System Administrator's Guide for UNIX*

  Explains how to configure and manage Storage Migrator on a UNIX system.

If your configuration includes Windows servers, you may also need the following manuals:

- *NetBackup Installation Guide for Windows*

  Explains how to install NetBackup DataCenter software on Windows-based platforms.

- *NetBackup DataCenter Media Manager System Administrator's Guide for Windows*

  Explains how to configure and manage storage devices and media in Media Manager. Media Manager is part of the NetBackup DataCenter product.

- *NetBackup DataCenter System Administrator's Guide for Windows*

  Explains how to configure and manage NetBackup DataCenter on a Windows server.

- *NetBackup Troubleshooting Guide for Windows*

  Provides troubleshooting information for Windows-based NetBackup DataCenter and BusinesServer products.

Accessibility

NetBackup contains features that make the user interface easier to use by people who are visually impaired and by people who have limited dexterity. Accessibility features include:

- Support for assistive technologies such as screen readers and voice input (Windows servers only)
- Support for keyboard (mouseless) navigation using accelerator keys and mnemonic keys

For more information, see the NetBackup system administrator's guide.

Conventions

The following explains typographical and other conventions used in this guide.

Type Style

Typographic Conventions

Typeface	Usage
`Bold fixed width`	Input. For example, type **`cd`** to change directories.
`Fixed width`	Paths, commands, filenames, or output. For example: The default installation directory is `/opt/VRTSxx`.
Italics	Book titles, new terms, or used for emphasis. For example: *Do not* ignore cautions.
Sans serif (italics)	Placeholder text or variables. For example: Replace *filename* with the name of your file.
Serif (no italics)	Graphical user interface (GUI) objects, such as fields, menu choices, etc. For example: Enter your password in the **Password** field.

Notes and Cautions

Note This is a Note. Notes are used to call attention to information that makes using the product easier or helps in avoiding problems.

Caution This is a Caution. Cautions are used to warn about situations that could cause data loss.

Key Combinations

Some keyboard command sequences use two or more keys at the same time. For example, holding down the **Ctrl** key while pressing another key. Keyboard command sequences are indicated by connecting the keys with a plus sign. For example:

Press Ctrl+t

Command Usage

The following conventions are frequently used in the synopsis of command usage.

brackets [ ]

The enclosed command line component is optional.

Vertical bar or pipe (|)

Separates optional arguments from which the user can choose. For example, when a command has the following format:

`command` *arg1*|*arg2*

the user can use either the *arg1* or *arg2* variable.

Terms

The terms listed in the table below are used in the VERITAS NetBackup documentation to increase readability while maintaining technical accuracy.

Term	Definition
Microsoft Windows, Windows	Terms used as nouns to describe a line of operating systems developed by Microsoft, Inc. A term used as an adjective to describe a specific product or noun. Some examples are: Windows 95, Windows 98, Windows NT, Windows 2000, Windows servers, Windows clients, Windows platforms, Windows hosts, and Windows GUI. Where a specific Windows product is identified, then only that particular product is valid with regards to the instance in which it is being used. For more information on the Windows operating systems that NetBackup supports, refer to the VERITAS support web site at `http://www.support.veritas.com`.
Windows servers	A term that defines the Windows server platforms that NetBackup supports; those platforms are: Windows NT and Windows 2000.
Windows clients	A term that defines the Windows client platforms that NetBackup supports; those platforms are: Windows 95, 98, ME, NT, 2000, XP (for 32- and 64-bit versions), and LE.

Getting Help

For updated information about this product, including system requirements, supported platforms, supported peripherals, and a list of current patches available from Technical Support, visit our web site:

```
http://www.support.veritas.com/
```

VERITAS Customer Support has an extensive technical support structure that enables you to contact technical support teams that are trained to answer questions to specific products. You can contact Customer Support by sending an e-mail to support@veritas.com, or by finding a product-specific phone number from the VERITAS support web site. The following steps describe how to locate the proper phone number.

1. Open `http://www.support.veritas.com/` in your web browser.
2. Click **Contact Support**. The *Contacting Support Product List* page appears.
3. Select a product line and then a product from the lists that appear. The page will refresh with a list of technical support phone numbers that are specific to the product you just selected.

Introduction 1

The Shared Storage Option (SSO) is a separately licensed and priced VERITAS option, and is available for NetBackup DataCenter only. This software option is the *Shared Drives* option and the license key used to enable it is the *Shared Drives* key.

SSO runs on Windows and UNIX servers (see “Supported Servers” on page 88).

SSO requires appropriate hardware connectivity, such as, fibre channel hubs or switches, SCSI multiplexors, or SCSI-to-fibre bridges (see “FAQ” on page 85).

What Is SSO?

SSO allows individual tape drives (stand-alone or in a robotic library) to be dynamically shared between multiple NetBackup media servers. Each media server can access any of the shared drives as needed and each server ”owns” the drives it has active. The shared drives are automatically allocated and deallocated as backup and restore operations dictate. This allows data to be backed up directly to tape drives in a SAN (Storage Area Network) configuration instead of moving data over the LAN—an important advantage of a SAN.

SSO Is An Extension of Media Manager

SSO is an important extension to tape drive allocation and configuration for NetBackup Media Manager (see “SSO Components in Media Manager” on page 88). NetBackup, Storage Migrator, and Storage Migrator Remote use Media Manager for configuration, allocation, and control of tape drives and robotic libraries.

SSO is a *software solution* (in NetBackup and Media Manager) and does not load firmware in SAN devices or communicate with hub or switch APIs. SSO can communicate with hub or switch APIs if the `shared_drive_notify` script is used.

A SAN Is Not Required for SSO

SSO provides the management and coordination tools necessary to effectively share tape resources in a SAN. SSO was designed to work with fibre channel networks, but it can also be applied to environments that use SCSI switches or multi-initiator configurations. SAN fibre is not required to use SSO.

SSO Related Terms and Concepts

When the Shared Storage Option is installed, a tape drive that is shared among hosts is termed a *shared drive*.

The VERITAS NetBackup Shared Storage Option is not the same as the VERITAS Backup Exec Shared Storage Option. The Backup Exec implementation of drive sharing does not include support for UNIX servers and uses a different method for drive arbitration.

Media Manager also manages distributed access from multiple servers to robotic tape libraries (*library sharing* or *robot sharing*). However, this capability is not related to SSO and should not be confused with SSO.

Sharing Drives Between NetBackup and Other Applications

There is no interoperability between NetBackup and Backup Exec SSO, and they can not share the same drives or robotics because of the different methods of drive arbitration that are used.

NetBackup also does not share devices with other applications running on a system. System commands that access drives that are configured in Media Manager (and are not in the down state) can interfere with device control and may lead to data loss.

Benefits of SSO

Sharing of Tape Drives

SSO dynamically shares tape drives across multiple heterogeneous hosts running NetBackup, increasing the utilization of tape drives and decreasing the total requirement for tape drives. Shared drives are managed across multiple servers as backup and restore operations dictate. In essence, SSO provides the ability to “move” tape drives to the backup or migration of data.

In a traditional environment where tape drives are directly SCSI-attached to a server platform, the resource-allocation environment is static. Tape drives may be up or down, but they can only be used by processes that are native to the media server.

In a SSO environment, every media server on the SAN can access the tape drives. SSO coordinates and assures sequential access to shared drives. Tape drives can be utilized more efficiently, because they don't have to be idle just because a single host is not using the drive (as in a traditional environment).

Takes Advantage of Fibre Channel

Allows fibre channel benefits, such as

- High data transfer rates.

  Faster backup speeds provide choices. Instead of providing more central servers to handle a pool of network clients, you can use SSO to get better performance on systems by having a pool of drives to be shared by your existing servers without dedicating tape drives to each system.

- Ability to route cables longer distances than with SCSI.
- Dynamic reconfiguration without disconnecting and reconnecting cables.

Reduces Storage Costs

Assume you have multiple large media servers, with each server requiring *n* drives to meet its backup window. If you can schedule these backup windows at different times, you can invest in only *n* drives, not *n* times the number of servers that are needed. Sharing hardware through SSO reduces storage costs.

Requires Fewer Drives for Restore Jobs

You may wish to reserve drives for restores. But reserving one drive per server in a traditional environment, might be more overhead than you want. With SSO, you can reserve *one* drive for all of your servers to share (see "Reserving a Drive for Restore Jobs" on page 62).

Provides Fault Tolerance

Assume you have a configuration with two servers sharing a library with two drives—one drive is SCSI-attached to each server. This is a typical Media Manager library sharing configuration. Now suppose one drive goes down. Without SSO, one of the servers can no longer backup and restore data. With SSO, both servers share the remaining drive, and backups and restores may just take longer than usual.

Provides Drive Resiliency

If a drive failure is detected from one server, NetBackup will initially down the drive only on that media server. Other media servers may still be able to access the drive. In other words, the drive is marked up or down on a media server basis.

Ability to Back Up to Locally-Attached Drives

SSO increases the number of situations where a platform that was formerly backed up as a NetBackup client can be configured as a NetBackup media server, and therefore gain the benefit of backing up to locally-attached tape drives. For Storage Migrator (or Storage Migrator Remote), SSO increases the number of situations where a platform that was using either of these products can be configured as a self-contained Storage Migrator.

In effect the hardware cost of increasing or restoring LAN capacity is the cost of adding SAN connectivity, not the cost of adding local tape drives.

How To Get SSO Installed and Running

Follow the basic steps outlined in the table below. The chapter references are to chapters in this guide.

Step	Task	Chapter Reference
1	Install and configure your SSO hardware. This includes SAN hardware and standalone equipment, as well as robots.	See “Installing and Configuring Your SSO Hardware” on page 11.
2	Verify your SSO hardware. Use operating system tools to test and verify your configuration. Make sure you can "see" your devices on the SAN network.	See “Verifying Your SSO Hardware Is Connected and Working” on page 27.
3	Install all software that is necessary for SSO operation. This includes installing SSO and NetBackup patches, and may include installing NetBackup (this includes Media Manager). A license key for SSO is also required.	See “Installing the Shared Storage Option” on page 29.
4	Configure SSO Use the Media Manager configuration wizards to configure robots and shared drives, and to add media to the Media Manager volume database.	See “Configuring SSO Devices and Media In Media Manager” on page 35.
5	Verify your SSO configuration. Use Media Manager utilities to resolve any problems or conflicts before putting your test SSO configuration into production.	See “Verifying Your SSO Configuration” on page 53.
6	Configure NetBackup to use SSO. Define NetBackup storage units and backup policies.	See “Configuring SSO Usage in NetBackup” on page 61.
7	Monitor your configuration. Use the SSO capabilities in Media Manager to check for problems, fine tune SSO, and to monitor your SSO devices.	See “Using SSO” on page 65.

What Are SAN and Fibre Channel?

The following background topics provide an overview of Storage Area Networks and fibre channel technology.

Storage Area Networks (SAN)

The building of networks between hosts and storage devices is called *storage networking*. A network used to connect hosts and storage devices is called a *storage area network (SAN)*. SAN is a term that has been adopted by the storage industry and refers to a network of multiple servers and storage devices connected together using fibre channel equipment. The commodity-like qualities of fibre channel components have caused a widespread adoption of this technology.

Disks, tape drives, and robots are commonly available with fibre channel interfaces. Devices with SCSI interfaces can also be used in a SAN with the addition of SCSI-to-fibre channel bridges (see “Fibre Channel Hardware” on page 8).

Tape devices have different usage characteristics from disk devices. Hosts generally maintain a continuous dialog with disk devices. Since this dialog for tape devices tends to be infrequent, SCSI-attached tape resources usually suffer poor utilization. Shared connectivity for tape devices on a SAN boosts utilization by treating these devices as shared resources.

Storage area network technology is gaining acceptance because it provides advantages over traditional SCSI-based connections. The chief advantage is ease of configuration. All hosts in a SAN can have equal visibility of all storage devices. From an operational standpoint, a variety of procedures can be completed without re-cabling the environment, as would be necessary using dedicated SCSI-attached devices.

Fibre Channel

Storage networking has been enabled by the performance and connectivity properties of fibre channel. *Fibre channel* is the name given to the assembly of physical interconnect hardware and the fibre channel protocol.

The basic connection to a fibre channel device is made by two serial cables, one carrying in-bound data and the other carrying out-bound data. Despite the name, fibre channel can run over fiber optic or twin-axial copper.

Fibre channel includes a communications protocol that was designed to accommodate both network-related messaging (such as IP traffic) and device-channel messaging (such as SCSI). True fibre-channel storage devices on a SAN are compatible with fibre channel protocol. Other devices on a SAN use SCSI protocol when communicating with a SCSI-to-fibre bridge.

Fibre Channel Topologies

Fibre channel protocol is designed to be low in overhead so it can function over a device channel, yet flexible so messages have addresses and can be efficiently switched. Devices that participate in fibre channel networking have names and identities. Fibre channel was designed to be as adept for carrying storage protocols (SCSI, HIPPI, and IPI) as carrying network protocols (IP and ATM).

At the lowest layers of the 5-layer protocol, fibre channel defines the following types of device connections.

Point-to-Point
This topology is the closest to a SCSI connection. It consists of two fibre channel devices connected directly together. The transmit fibre of one device goes to the receive fibre of the other device, and vice versa. There is no sharing of the media, so the devices enjoy the total bandwidth of the link. A link initialization is required of the two devices before communication can begin.
Arbitrated Loop (FC-AL)
This is the most dominant fibre channel topology because of low cost, but is falling out of favor because of poor performance. This topology allows up to 126 devices to reside on a physical loop. Any device on the loop must negotiate access to the loop in order to transfer data. The media is shared among the devices, limiting each device's access. Arbitrated loops are private in that devices on the loop are only visible to the host where the loop is connected and only a minimal self-identification procedure is conducted at system startup.
Switched Fibre Channel (Fibre Channel Fabric or Fabric)
This topology is used to connect many (up to 2^{24}) devices in a cross-point switched configuration. The benefit of this topology is that many devices can communicate at the same time and the media can be shared. It also requires fibre channel switches.

Fibre Channel Addresses

There are a number of different types of addresses that may be used within a fibre channel network.

World Wide Name (WWN)
A unique identifier that is assigned to each node and port in a fibre channel network.
Arbitrated Loop Physical Address (ALPA)

One of 126 non-contiguous single-byte numbers, which is assigned to a device on a fibre channel arbitrated loop.
Arbitrated Loop Number
A number between 0 and 125, which maps to one of the 126 ALPAs.
Fibre Channel Logical Unit Number (FC LUN)
A number assigned to devices which share a common ALPA.

Fibre Channel Hardware

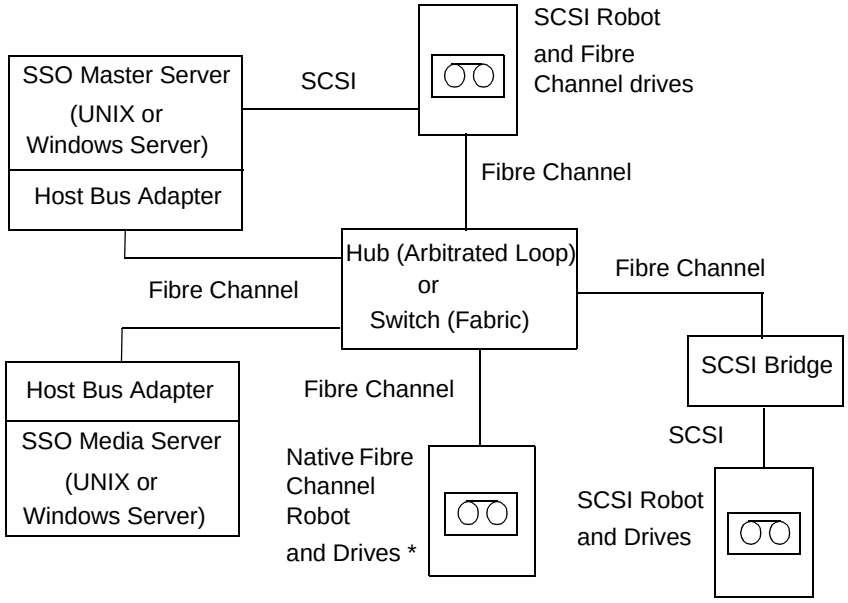
Common fibre channel hardware includes the following.

Fibre Channel Hub
A hub is an appliance with many fibre channel ports. Internally, the hub connects all the ports together into a loop topology. Hubs are tools for connecting fibre channel devices together into an arbitrated loop.
Fibre Channel Switch
At startup time, every device or host on a fabric network must log on providing an identity and an address. Fibre channel switches catalog the names of all visible devices and hosts, and are able to direct messages between any two points in the network. Switches can be interconnected in ring or cascaded tree configurations to increase the number of device connections or to increase the bandwidth between designated points in the network. Redundant fabric for high-availability environments is constructed by connecting multiple switches to multiple hosts.
Host Bus Adapters (HBA)
These components link servers to fibre channel. HBAs are usually separate cards in the server. Initially, fibre channel HBAs emulated SCSI-2 parallel interfaces to work with existing system drivers (in most cases). Native fibre channel HBAs using SCSI-3 protocol are now available and these HBAs may not be compatible with these older drivers.
SCSI Bridges (or Routers)
Devices with SCSI interfaces can be connected to a fibre channel network using a SCSI-to-fibre bridge. A bridge converts SCSI protocol to fibre channel protocol. Several manufacturers offer bridges that can be used to connect SCSI tape drives and robots to a fibre channel network. A SCSI-to-fibre bridge is also known as a fibre router.

SAN Component Example

The following figure shows typical SAN components in a shared drive configuration.

Example SAN Configuration



* Some robots have integrated bridges, but native fibre channel devices do not.

Installing and Configuring Your SSO Hardware 2

SSO hardware configuration involves the following:

- Configuring your SAN environment.
- Attaching robots and drives.
- Getting servers to recognize these devices.

On Windows servers, attaching devices and getting the system to recognize these devices is usually done by the operating system (in some instances you may have to install device drivers). On UNIX servers such as on Sun Solaris, hardware configuration may be more involved, including modifying the sg driver configuration and other configuration files.

See the figure “Example SAN Configuration” on page 9 for a SAN terminology and configuration overview.

General Procedure

Some of the following tasks may be optional depending on your particular hardware configuration.

See “Example Fibre Channel Configuration” on page 22 for a more detailed example of configuring hardware for SSO on a Solaris host.

- Determine the physical location of each drive within the robot.

Note This task may not be needed if you are able to use device discovery (a part of the device configuration wizard). See “Device Configuration Wizard” on page 36.

  This is usually shown on the connectors to the drives or in the vendor documentation. The robot and slot layout appendix in the Media Manager system administrator’s guide shows the layout for many of the robots that Media Manager supports.

- Make all drive and robot hardware connections.
- Install SAN connecting hardware (for example, bridges, switches, routers, or hubs).
- If fibre is part of your configuration and you are using a SCSI-to-fibre bridge, determine the SCSI-to-fibre channel mapping for your tape devices.

Hard-wired SCSI IDs are converted to fibre channel LUNs that are presented to hosts involved in the configuration. Understanding which LUNs map to which physical SCSI IDs will ensure correct drive assignments. See “Fibre Channel Mapping Examples” on page 16.

Familiarity with the hardware and various vendor configuration tools will help you accomplish this. See the vendor documentation for your bridge.

- Record the physical configuration.

  When setting up an SSO configuration, it is helpful to record your hardware information. Record the adapter, SCSI addresses, WWNs, and fibre channel LUNs to which you connected each drive. It is also useful to record the version levels of firmware and drivers. For examples, see “Example SSO Configuration Matrix” on page 15 and the tables in “Fibre Channel Mapping Examples” on page 16.

- Install and configure the appropriate drivers.

  See your vendor documentation for instructions.

- On UNIX servers, create any device files that are needed. Depending on the operating system, these may be created automatically by using a reconfiguration reboot (`boot -r`).

  Create the device files for each drive based on the fibre channel LUNs of the drives and adapters. Add the name of the device file to your notes to complete the correlation between device files and physical drive location.

  Use the device configuration guide (see “Using the Media Manager Device Configuration Guide” on page 14) and the man pages that are available with the operating system.

- On UNIX servers, customize the operating system by modifying the appropriate system configuration files. This task requires knowledge of the system files that use the SSO environment and their formats.

  For example on Sun Solaris systems, you may need to modify the sg and HBA driver files. See the Sun chapter of the NetBackup Media Manager device configuration guide.

  Modify the HBA driver files to bind fibre channel devices (WWN) to a specific target ID. See your vendor documentation for specific syntax and more information.

- On Windows servers, refer to the HBA documentation from the vendor for instructions on configuring the HBA.

- Use the configuration interface available for each piece of hardware you are using to configure and ensure that the configuration is what you expect.

  For example on Windows servers, you can use the HyperTerminal interface to configure SCSI-to-fibre bridges (click **Start - Programs - Accessories - HyperTerminal**).

Use the following general order when you configure and verify the hardware (start with the robot and shared drives and work back to the host):

a. Robot and shared drives

b. Bridges

c. Hub or switches

d. Hosts

- If you experience errors during the installation and configuration of your SSO devices and you suspect the operating system, refer to the operating system logs as described in your operating system documentation.

Windows Hosts

Device Drivers

If you need to install tape device drivers, VERITAS recommends using the Windows tape drivers and installer found on the support web site. You can download the latest tape drivers and tape installer from `http://support.veritas.com`.

Search on the keywords *tape device installer*. These drivers support the tape devices listed in the compatibility lists on this web site.

`NetBackupTapeDeviceDriverInstall`.exe will run only if NetBackup has been installed.

Logical to Physical Mapping

Record the Windows tape device entries (logical to physical mapping) as follows. Also see “Example SSO Configuration Matrix” on page 15 and the tables in “Fibre Channel Mapping Examples” on page 16.

Note The following steps may not be needed if you are able to use device discovery (a part of the device configuration wizard). See “Device Configuration Wizard” on page 36.

1. Note the fibre channel LUN assigned to the drive, and check the Windows **Tape Devices** display from the **Control Panel** to determine which device name (for example, `Tape0`) was assigned to the drive.

2. Correlate the SCSI target to the robot drive number by using the robot's interface panel or checking the indicators on the rear panel of the tape drive.

3. Determine the physical drive number by checking labels on the robot itself or by using the robot and slot layout appendix in the Media Manager system administrator's guide. This appendix shows the layout for many of the robots that Media Manager supports.

Multiple Devices

If you have multiple devices connected to a fibre router, Windows may only see one LUN. This will normally be the device with the lowest-ordered LUN.

This limitation occurs because of the default install settings for the device driver for some fibre channel HBAs. See your vendor documentation to verify the settings.

UNIX Hosts

Using the Media Manager Device Configuration Guide

See the *NetBackup Media Manager Device Configuration Guide for UNIX* for information on installing and configuring drivers, and modifying the appropriate system configuration files.

The configuration tasks explained in the device configuration guide are quite similar to the tasks required when configuring an SSO environment and in some cases specific fibre channel changes may be explained.

Solaris Configurations

See the Sun4/SPARC chapter of the NetBackup Media Manager device configuration guide. This chapter also contains information about the modifications needed in the sg driver configuration to detect SCSI LUNs greater than 1 and SCSI targets greater than 7. This change is often needed for fibre-attached devices.

Minimize the number of entries in the `sg.conf` file to minimize the time needed for the following:

- System boot
- Device discovery
- `sgscan`

SSO Configurations With More Than 16 Tape Drives

Changes in tape device status may not be visible to all media servers in an SSO configuration if there are more than 16 tape devices configured.

When the number of tape devices configured approaches 16, the default maximum size of Solaris IPC message queues may not be large enough. In these cases, communication between the `rdevmi` process on scan hosts and `oprd` processes on media servers can be interrupted when the number of messages sent exceeds the maximum size of the queue.

VERITAS recommends adding the following statement to the `/etc/system` file. This statement sets the maximum number of bytes in an IPC message queue to 65536. A reboot is necessary for the statement to take effect.

```
set msgsys:msginfo_msgmnb=65536
```

Be aware that increasing the maximum size of the IPC message queue may increase the amount of memory allocated to other IPC message queues on the same system It is recommended that the impact of this change should be fully assessed before it is implemented.

Example SSO Configuration Matrix

It may be helpful to record your physical configuration. You can complete a configuration matrix similar to the following example:

1	2	3	4	5	6	7	8	9
Physical Definition	**Physical SCSI ID At Library**	**Physical Bus ID At Switch**	**Logical Fibre Channel To LUN Mapping**	**Fibre Channel WWN**	**Device Name On Windows**	**Device Name On UNIX Host**	**Pass-thru Path On Solaris Host**	**Logical NetBackup Storage Unit Name**

In column	Identify and record the
1	Equipment type.
2	Physical SCSI ID of each piece of equipment.
3	Physical bus number where the equipment is attached.
4	SCSI to LUN mapping assignments. Log into the bridge to obtain these mappings.
5	World Wide Name of fibre channel port or node (on Solaris hosts only).
6	Device name used by the Windows host.
7	Device path used by the UNIX host.
8	Pass-thru path used by sg driver (on Solaris hosts only).
9	Logical storage unit name used by NetBackup.

Fibre Channel Mapping Examples

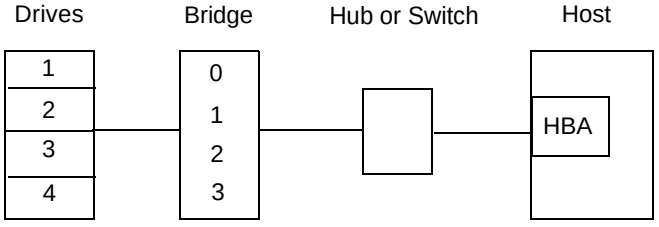
The following examples contain SCSI-to-fibre bridges and show the SCSI-to-fibre channel mappings in various configurations.

In these examples

- HBA is a host bus adapter.
- FC LUN is a fibre-channel LUN.
- UNIX (Sun Solaris) and Windows are the example platforms.
- The pass-thru paths for Solaris (shown in column 6 in the tables) do not need to start at c0. The paths shown are only examples and can be any adapter number. These paths are used when configuring the NetBackup sg driver on Solaris hosts.
- Examples 4, 5, and 6 have two HBAs in the configurations. Since the operating system recognizes two paths to each drive, this results in two hardware paths for each tape device. You must choose one of the two paths available for each tape device, since only one path for each device can be configured in Media Manager.

Example 1

This example consists of four tape drives, a SCSI-to-fibre bridge, a hub or switch, and a host bus adapter.



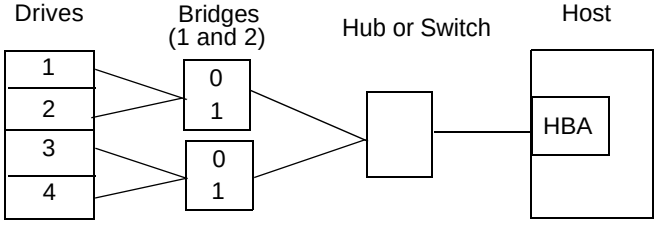
The following table shows the device names and the device paths that you would use when configuring the drives in this configuration.

One Bridge - One HBA

Drive (SCSI ID)	FC LUN	SCSI Coordinates (Port Bus Target LUN)	Device Name (Windows)	Device Path (UNIX)	Pass-thru Path (Solaris)
1	0	0 0 0 0	Tape0	/dev/rmt/0cbn	/dev/sg/c0t0l0
2	1	0 0 0 1	Tape1	/dev/rmt/1cbn	/dev/sg/c0t0l1
3	2	0 0 0 2	Tape2	/dev/rmt/2cbn	/dev/sg/c0t0l2
4	3	0 0 0 3	Tape3	/dev/rmt/3cbn	/dev/sg/c0t0l3

Example 2

This example consists of four tape drives, two SCSI-to-fibre bridges, a hub or switch, and a host bus adapter. SCSI IDs 1 and 2 are on bridge 1. SCSI IDs 3 and 4 are on bridge 2. Bridge 1 was discovered first by the operating system.



The following table shows the device names and the device paths that you would use when configuring the drives in this configuration.

Two Bridges - One HBA - Bridge 1 Discovered First

Drive (SCSI ID)	FC LUN	SCSI Coordinates (Port Bus Target LUN)	Device Name (Windows)	Device Path (UNIX)	Pass-thru Path (Solaris)
1	0	0 0 0 0	Tape0	/dev/rmt/0cbn	/dev/sg/c0t0l0
2	1	0 0 0 1	Tape1	/dev/rmt/1cbn	/dev/sg/c0t0l1
3	0	0 0 1 0	Tape2	/dev/rmt/2cbn	/dev/sg/c0t1l0
4	1	0 0 1 1	Tape3	/dev/rmt/3cbn	/dev/sg/c0t1l1

Because bridge 1 was discovered first, the drive with the SCSI ID of 1 is assigned the first available device name and device path (see the first row in the table).

Example 3

This example uses the same configuration as shown in “Example 2” on page 17. However in this example, bridge 2 was discovered first by the operating system.

The following table shows the device names and the device paths that you would use when configuring the drives in this configuration.

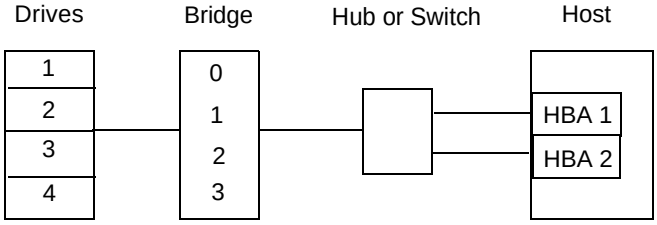
Two Bridges - One HBA - Bridge 2 Discovered First

Drive (SCSI ID)	FC LUN	SCSI Coordinates (Port Bus Target LUN)	Device Name (Windows)	Device Path (UNIX)	Pass-thru Path (Solaris)
1	0	0 0 1 0	Tape2	/dev/rmt/2cbn	/dev/sg/c0t1l0
2	1	0 0 1 1	Tape3	/dev/rmt/3cbn	/dev/sg/c0t1l1
3	0	0 0 0 0	Tape0	/dev/rmt/0cbn	/dev/sg/c0t0l0
4	1	0 0 0 1	Tape1	/dev/rmt/1cbn	/dev/sg/c0t0l1

Since bridge 2 was discovered first, the drive with the SCSI ID of 3 is assigned the first available device name and device path (see the third row in the table).

Example 4

This example consists of four tape drives, a SCSI-to-fibre bridge, a hub or switch, and two host bus adapters.



The following table shows the device names and the device paths that you could use when configuring the drives in this configuration.

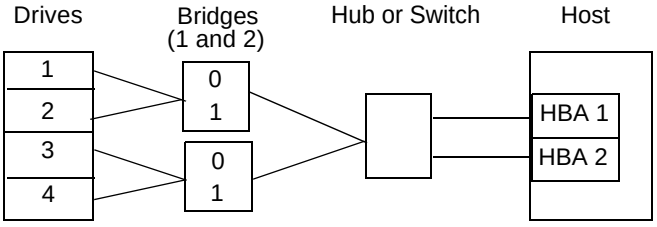
One Bridge - Two HBAs

Drive (SCSI ID)	FC LUN	SCSI Coordinates (Port Bus Target LUN)	Device Name (Windows)	Device Path (UNIX)	Pass-thru Path (Solaris)
1	0	0 0 0 0	Tape0	/dev/rmt/0cbn	/dev/sg/c0t0l0
2	1	0 0 0 1	Tape1	/dev/rmt/1cbn	/dev/sg/c0t0l1
3	2	0 0 0 2	Tape2	/dev/rmt/2cbn	/dev/sg/c0t0l2
4	3	0 0 0 3	Tape3	/dev/rmt/3cbn	/dev/sg/c0t0l3
1	0	1 0 0 0	Tape4	/dev/rmt/4cbn	/dev/sg/c1t0l0
2	1	1 0 0 1	Tape5	/dev/rmt/5cbn	/dev/sg/c1t0l1
3	2	1 0 0 2	Tape6	/dev/rmt/6cbn	/dev/sg/c1t0l2
4	3	1 0 0 3	Tape7	/dev/rmt/7cbn	/dev/sg/c1t0l3

Because of the second HBA, the operating system recognizes two paths to each drive resulting in two hardware paths for each tape device. You must choose one of the two paths available for each tape drive when configuring the drives in Media Manager.

Example 5

This example consists of four tape drives, two SCSI-to-fibre bridges, a hub or switch, and two host bus adapters. SCSI IDs 1 and 2 are on bridge 1. SCSI IDs 3 and 4 are on bridge 2. Bridge 1 was discovered first by the operating system.



The following table shows the device names and the device paths that you could use when configuring the drives in this configuration.

Two Bridges - Two HBAs - Bridge 1 Discovered First

Drive (SCSI ID)	FC LUN	SCSI Coordinates (Port Bus Target LUN)	Device Name (Windows)	Device Path (UNIX)	Pass-thru Path (Solaris)
1	0	0 0 0 0	Tape0	/dev/rmt/0cbn	/dev/sg/c0t0l0
2	1	0 0 0 1	Tape1	/dev/rmt/1cbn	/dev/sg/c0t0l1
3	0	0 0 1 0	Tape2	/dev/rmt/2cbn	/dev/sg/c0t1l0
4	1	0 0 1 1	Tape3	/dev/rmt/3cbn	/dev/sg/c0t1l1
1	0	1 0 0 0	Tape4	/dev/rmt/4cbn	/dev/sg/c1t0l0
2	1	1 0 0 1	Tape5	/dev/rmt/5cbn	/dev/sg/c1t0l1
3	0	1 0 1 0	Tape6	/dev/rmt/6cbn	/dev/sg/c1t1l0
4	1	1 0 1 1	Tape7	/dev/rmt/7cbn	/dev/sg/c1t1l1

Because of the second HBA, the operating system recognizes two paths to each drive resulting in two hardware paths for each tape device. Since bridge 1 was discovered before bridge 2, the device names and device paths are the same as in “Example 4” on page 19; however, adding a second bridge causes the FC LUN and SCSI coordinates to change.

You must choose one of the two paths available for each tape drive when configuring the drives in Media Manager.

Example 6

This example uses the same configuration as shown in “Example 5” on page 20. However in this example, bridge 2 was discovered first by the operating system.

The following table shows the device names and the device paths that you could use when configuring the drives in this configuration.

Two Bridges - Two HBAs - Bridge 2 Discovered First

Drive (SCSI ID)	FC LUN	SCSI Coordinates (Port Bus Target LUN)	Device Name (Windows)	Device Path (UNIX)	Pass-thru Path (Solaris)
1	0	0 0 1 0	Tape2	/dev/rmt/2cbn	/dev/sg/c0t1l0
2	1	0 0 1 1	Tape3	/dev/rmt/3cbn	/dev/sg/c0t1l1
3	0	0 0 0 0	Tape0	/dev/rmt/0cbn	/dev/sg/c0t0l0
4	1	0 0 0 1	Tape1	/dev/rmt/1cbn	/dev/sg/c0t0l1
1	0	1 0 1 0	Tape6	/dev/rmt/6cbn	/dev/sg/c1t1l0
2	1	1 0 1 1	Tape7	/dev/rmt/7cbn	/dev/sg/c1t1l1
3	0	1 0 0 0	Tape4	/dev/rmt/4cbn	/dev/sg/c1t0l0
4	1	1 0 0 1	Tape5	/dev/rmt/5cbn	/dev/sg/c1t0l1

Because of the second HBA, the operating system recognizes two paths to each drive resulting in two hardware paths for each tape device. Since bridge 2 was discovered before bridge 1, the device names, device paths, and the SCSI coordinates have changed from those shown in “Example 5” on page 20.

You must choose one of the two paths available for each tape drive when configuring the drives in Media Manager.

Example Fibre Channel Configuration

This example is taken from NetBackup configuration lab testing at VERITAS.

Hardware Components in This Example

- UNIX Solaris 2.6, 7, or 8 host
- JNI HBA
- Brocade 2400 switch
- Compaq Fibre Channel Tape Controller II
- Compaq TL895 tape library

Files Changed in This Example

NetBackup

- `/usr/openv/volmgr/bin/driver/sg.conf`
- `/usr/openv/volmgr/bin/driver/sg.links`

Operating System

- `/kernel/drv/st.conf`

HBA-Specific

The actual file changed depends on which HBA driver is used.

- `/kernel/drv/fca(w).conf`

Steps To Configure the Hardware

1. Use the serial connection to the bridge to confirm that the bridges can see the robot controller and all the drives. For this Compaq fibre-channel tape controller configuration, use menu item **1) Display Currently Attached SCSI Devices**. Output from the two bridges in this configuration follows. In this example, bridge 1 can see the robot controller (`DESCRIPTION TL810`) and three drives. Bridge 2 can see two drives.

```
Currently Attached Devices
   Build Level: c9909p

BUS TGT LUN DEVICE DESCRIPTION
 0   1   0  DEC     TL810        (C) DEC2.31
 0   2   0  DEC     TZ89         (C) DEC2150
 0   3   0  DEC     TZ89         (C) DEC2150
 1   2   0  DEC     TZ89         (C) DEC2150

BUS TGT LUN DEVICE DESCRIPTION
 0   3   0  DEC     TZ89         (C) DEC2150
 0   4   0  DEC     TZ89         (C) DEC2150
```

View of the devices for Bridge 1.

View of the devices for Bridge 2.

2. Display the SCSI-to-fibre channel mapping on the bridges. In this configuration, go to the maintenance menu (enter **maint** at the first menu) on either of the bridges. Use option **3) Display FC to SCSI Mapping**. The output is the same for each of the bridges.

```
Fibre Channel to SCSI Display
    Build Level: c9909p

FC_LUN       BUS TGT LUN
 0x00   ->    0   0   0
 0x01   ->    0   1   0
 0x02   ->    0   2   0
 0x03   ->    0   3   0
 0x04   ->    1   1   0
 0x05   ->    1   2   0
 0x06   ->    1   3   0
 0x07   ->    1   0   0
 0x08   ->    0   4   0
 0x09   ->    0   5   0
 0x0A   ->    0   6   0
 0x0B   ->    1   4   0
 0x0C   ->    1   5   0
 0x0D   ->    1   6   0
 0x0E   ->    0   8   0
 0x0F   ->    1   8   0
```

In this example, these are the five relevant entries that match the BUS, TGT, and LUN of the devices that are connected. See the device output displayed in step 1.

3. Bind the WWN for the device to an arbitrary target number. The world wide name of the bridges can be found on the bridge or in the boot-time messages that are written to the `/var/adm/messages` log on the Solaris server.

   The binding procedure is HBA-vendor specific. JNI adapters can be configured using ezfibre (a JNI product). Other HBAs can be configured by adding entries in their respective `.conf` files.

   For this example, assume bridge 1 is bound to target 0 and bridge 2 to target 1. The `/kernel/drv/fcaw.conf` file would have the following entries created by ezfibre:

```
name="fcaw" parent="/sbus@1f,0"
reg=1, 0x0, 8000, 1, 0x8000, 8000, 1, 0x10000, 2, 1, 0x20000,
   4, 1, 0x30000, 200
target0_wwnn="500508b3000000b9"
target0_hba="fcaw0"
target1_wwnn="500508b3000000d6"
target1_hba="fcaw0"
def_hba_binding="null";
```

4. For each of the FC_LUNs with the BUS, TGT, and LUN values matching the devices that the bridges display, add entries in the `/usr/openv/volmgr/bin/driver/sg.links` file, so that the necessary `/dev/sg/*` nodes are created. These are the five FC_LUNs noted in step 2.

   The entries that follow are for bridge 1. For the four devices on this bridge, FC_LUNs 1, 2, 3, and 5 are needed.

```
type=ddi_pseudo;name=sg;addr=0,1;       sg/c\N0t0l1
type=ddi_pseudo;name=sg;addr=0,2;       sg/c\N0t0l2
type=ddi_pseudo;name=sg;addr=0,3;       sg/c\N0t0l3
type=ddi_pseudo;name=sg;addr=0,5;       sg/c\N0t0l5
```

   The entries that follow are for bridge 2. For the two drives on this bridge, FC_LUNs 3 and 8 are needed.

```
type=ddi_pseudo;name=sg;addr=1,3;       sg/c\N0t1l3
type=ddi_pseudo;name=sg;addr=1,8;       sg/c\N0t1l8
```

Note The target and luns in the address part of the `devlink.tab` entries are hexadecimal, but they are decimal in the `sg/c\N0tmln` part of the entries. Also, make sure that there are tabs between the columns, not spaces.

5. Add additional target and lun entries for each device to the `/usr/openv/volmgr/bin/driver/sg.conf` file.

   The entries that follow are for bridge 1:

```
name="sg" class="scsi" target=0 lun=1;
```

```
name="sg" class="scsi" target=0 lun=2;
name="sg" class="scsi" target=0 lun=3;
name="sg" class="scsi" target=0 lun=5;
```

The entries that follow are for bridge 2:

```
name="sg" class="scsi" target=1 lun=3;
name="sg" class="scsi" target=1 lun=8;
```

6. Add (or un-comment) the appropriate drive entries in the `tape-config-list` and add (or un-comment) the matching `data-property-name` entry in the `/kernel/drv/st.conf` file.

```
tape-config-list =

"DEC     TZ89",          "DEC DLT",               "DLT7k-data";

DLT7k-data = 1,0x38,0,0x19639,4,0x82,0x83,0x84,0x85,2;
```

7. Add name entries to the `/kernel/drv/st.conf` file.

```
name="st" class="scsi" target=0 lun=1;
name="st" class="scsi" target=0 lun=2;
name="st" class="scsi" target=0 lun=3;
name="st" class="scsi" target=0 lun=5;
name="st" class="scsi" target=1 lun=3;
name="st" class="scsi" target=1 lun=8;
```

8. Remove the old `sg.conf` file.

```
rm -r /kernel/drv/sg.conf
```

9. Run the `/usr/openv/volmgr/bin/driver/sg.install` script to copy the files into the correct locations.

10. Use `boot -r` to reboot the operating system and `/usr/openv/volmgr/bin/sgscan` to display the devices.

Verifying Your SSO Hardware Is Connected and Working 3

Test your hardware configuration before proceeding with other configuration steps—this task is very important and is often overlooked. Note the following points:

- Verify that all of your servers (master and media) are able to communicate with one another. Perform a `ping` from each server to every other server. Be sure to `ping` by host name to verify that the name resolution methods are functioning properly.
- Use the NetBackup `bpclntcmd` utility to resolve IP addresses into host names. See the NetBackup troubleshooting guide and the NetBackup system administrator's guide for more information.
- Make sure that robots and shared drives are visible to your operating system (for example on Solaris, use `mt -f /dev/rmt/0 status`). If it doesn't work for the operating system, it won't work for SSO.
- Make sure any dip switches on drives are set correctly (see "SSO Restrictions and Limitations" on page 31).

Verifying Your Configuration On UNIX Hosts

Use operating system and Media Manager commands and tools where available to verify the devices are configured correctly. Make sure you can "see" your devices on the SAN before you install and configure the SSO option.

Host Type	OS Command	Media Manager Command
Solaris	mt	/usr/openv/volmgr/bin/sgscan
IRIX	/usr/sbin/hinv	/usr/openv/volmgr/bin/mmscan
AIX	smit /usr/sbin/lsdev	
Tru64	/sbin/hwmgr	/usr/openv/volmgr/bin/lsdev

Host Type	OS Command	Media Manager Command
HP-UX	sam ioscan -f	
DYNIX/ptx	/etc/dumpconf /etc/showcfg	

See the appropriate chapter in the NetBackup Media Manager device configuration guide for more information and examples of usage (the chapters are organized by host type).

Verifying Your Configuration On Windows Hosts

From the Windows **Control Panel**, use the **Tape Devices** and **SCSI Adapters** interfaces or use `regedit`.

The path for registry entries for SCSI devices follows:

HKEY_LOCAL_MACHINE > HARDWARE > DEVICEMAP > SCSI

Installing the Shared Storage Option 4

This chapter covers requirements, restrictions, and the installation of SSO.

System Requirements for SSO

General System Requirements

Because control messages used by the device allocator and many types of robot control are passed by a socket connection, all NetBackup and Storage Migrator (or Storage Migrator Remote) servers must be LAN-connected.

NetBackup Media Manager Versions

Confirm that the same release and patch levels of NetBackup (and therefore Media Manager) are installed on all hosts that will be sharing drives.

NetBackup release 3.4 or later is required if you want to use the features of the following wizards:

- The device configuration wizard (see “Device Configuration Wizard” on page 36).
- The volume configuration wizard (see “Using the Volume Configuration Wizard to Configure Media” on page 48).

VERITAS Patch Levels

Ensure that all of your media servers have the latest VERITAS NetBackup jumbo patch installed. See “Where to Go for More Information” on page 92 for the VERITAS support web site.

Volume Database Host (Device Allocation Host)

The host that is defined as the volume database host (usually the NetBackup Master Server) is also the device allocation host for the SSO feature. If this system fails, not only will the SSO feature become non-operational, but all NetBackup backup and restore activity will fail. The following are requirements and recommendations for this host.

Host Requirements
It must be network-accessible from all hosts that are sharing drives managed by that device allocation host.
It must be running the same version of NetBackup as the hosts that are sharing drives managed by that device allocation host.
VERITAS Host Recommendations
Use a common volume database host (the NetBackup Master Server is recommended) for your configuration.
Configure the common volume database host as a Highly Available host.
Use a relatively high-powered server for your volume database host.

Windows System Requirements

On the System Where You Install SSO
VERITAS NetBackup DataCenter Release 3.2 or later software installed. Release 3.4 or later is required if you are running Windows 2000.
200 MHz or faster CPU.
64MB of RAM.
50 MB of disk space available for virtual memory paging.

UNIX System Requirements

On the System Where You Install SSO
VERITAS NetBackup DataCenter Release 3.2 or later software installed.
The UNIX system must be running an operating system level that is one of the system levels supported as a VERITAS NetBackup server.

SSO Restrictions and Limitations

- SSO cannot be used to share drives with the following:
  - An NDMP server. For example, a Network Appliance or an Auspex file server (both NDMP servers) cannot share a tape drive with a NetBackup media server.
  - VERITAS Backup Exec.
  - Other applications running on a system, including system commands that access shared drives. This can interfere with device control and may lead to data loss.
- SSO cannot be used with
  - Certain types of tape robots. See “Supported Robot Types” on page 87 for more information on the robot types that are supported.
  - Robots that are under the control of Microsoft’s Removable Storage Manager (RSM).
- SSO is configured with Media Manager interfaces that are provided with NetBackup. If you intend to utilize SSO with VERITAS Storage Migrator (or Storage Migrator Remote), you also must have NetBackup installed.
- Frequency-based drive cleaning is not supported for SSO drives. TapeAlert should be used (see the reference topics appendix of the NetBackup Media Manager system administrator’s guide for more information). Also see “FAQ” on page 85.
- Fibre channel I/O requires enhanced error recovery handling. This handling is currently available only on limited host platforms.
- Fibre channel technology is quite new. Operating systems provided by host vendors have not been fully developed in dealing with error situations. In particular, individual host power failure or reboots can affect data transfers on other hosts that share connectivity on a SAN.

- NetBackup does not share media between media servers for shared (or non-shared) drives. When media is first used in a backup, NetBackup notes the media server where the media is written and does not allow the media to be used by other servers.
- Sony AIT tape drives *may* require specific dip switch settings for proper SSO configuration and these settings can be different on various hosts. This is a limitation in their use in a SSO configuration. A Sony AIT drive cannot be connected to multiple hosts that require different switch settings. In homogeneous configurations these drives work fine; for example, in a configuration with multiple Windows hosts or multiple Solaris hosts.
  - For Windows hosts, the settings for dip switches 1-4 should be left at the default setting (all Off).
  - For UNIX hosts, see the appropriate chapter in the NetBackup Media Manager device configuration guide for your host to see if you need to change the switch settings.

SSO Installation

When you install NetBackup on a server you enter a key for the base NetBackup product. When the base NetBackup software is installed, Media Manager and the Shared Storage Option software are also installed.

SSO is a separately licensed feature and although the SSO software is installed, you need a key to enable it. Check the license keys that were included with your software order to ensure that you have the Shared Drives key.

On the server you are also prompted to enter license keys for any other product options that you purchased and want to enable. For more information on administering licenses, see the NetBackup DataCenter system administrator's guide.

Enable SSO on All Servers

SSO must be enabled (by entering the shared drives key) on every server where shared drives will be configured and used. You should do the following:

1. Enable SSO on your master server.
2. Enable SSO on all of your media servers.

Using the STK SN6000 With NetBackup

StorageTek (STK) introduced the SN6000 (Storagenet 6000 Storage Domain Manager) as a method for providing tape drive virtualization. Logical tape drives are presented to host operating system interfaces (tape drivers), while robotic control is accomplished through the Automated Cartridge System (ACS) API.

VERITAS supports configurations with the SN6000 using NetBackup release 3.4 and later releases. To avoid operational issues with the SN6000, a NetBackup patch is required.

Shared Drives License Key Required

To use the SN6000 with NetBackup, you need to enter the Shared Drives license key on each media server where ACS drives in the SN6000 are configured.

For more information on configuring the SN6000, see the ACS appendix in either of the following guides:

- *NetBackup DataCenter Media Manager System Administrator's Guide for UNIX*.
- *NetBackup DataCenter Media Manager System Administrator's Guide for Windows.*

Configuring SSO Devices and Media In Media Manager 5

This chapter explains what you need to do from NetBackup and Media Manager interfaces to configure SSO.

Why You Should Use the NetBackup Wizards

The recommended and easiest method for configuring shared drives is to use the NetBackup wizards, but there are alternate ways that are available (see “Using Alternate Interfaces for SSO Device Configuration” on page 50).

In addition to making setup faster, the wizards eliminate many common mistakes made when SSO configuration is done using alternate methods.

Use the NetBackup wizards as follows:

1. From your master server, use one of the device configuration wizards to configure robots and shared drives.

   See “Using the Device Configuration Wizards” on page 36.

2. After configuring a subset of shared devices, use the configuration analyzer to point out any errors before continuing configuring other devices.

   See “Media and Device Management Configuration Analyzer” on page 67.

3. Run the Volume Configuration wizard to configure media for robots and standalone drives.

   See “Using the Volume Configuration Wizard to Configure Media” on page 48.

Using the Device Configuration Wizards

Caution Use these wizards with care in a production environment, since the wizards stop the Media Manager daemons/services. You should not be running production backups when using these wizards.

Depending on the robot type you want to configure, use one of the following wizards.

To Configure	Use This Wizard
TL8, TLD, or TLH robots Drives in TL8, TLD, or TLH robots Standalone drives	See "Device Configuration Wizard" on page 36 and note the server platform limitations in "Wizard Limitations" on page 38.
Drives in ACS or TLM robots Standalone drives	See "Shared Drive Wizard" on page 45.

These wizards are available from the Media and Device Management interface of the NetBackup Administration GUI. This interface is available with the following NetBackup products:

- NetBackup for Windows servers
- NBJava (`jnbSA`) on supported UNIX servers

Note Some wizard screens differ slightly on Windows and UNIX versions of NetBackup.

Device Configuration Wizard

This wizard should be run on a media server (this server is usually the master server) with a limited number of devices during testing.

This wizard performs device discovery, and adds robotic libraries and shared drives to your Media Manager configuration. To perform these tasks, this wizard uses device serialization (also see "Wizard Limitations" on page 38).

Device Serialization

Many robots and drives support device serialization. Device serialization is a firmware feature that allows device identification and configuration. If the device supports serialization, the following happens when the wizard queries the devices in your configuration:

- Each robot and drive found in the configuration returns a unique serial number.
- For any robots in the configuration, an additional command is issued to the robot. The robot returns the number of drives and the serial number for each of the drives contained in the robot. This information is used by the wizard to determine the correct drive number for each drive in the robot.

Since device serialization is a relatively new capability for some devices, you may need to ask your hardware vendor for newer firmware that returns serial numbers. Even with the proper firmware, some devices require the vendor to perform another action to enable serialization for the device.

If a vendor releases firmware to support serialization after a NetBackup release, VERITAS may need to make changes to take advantage of any new serialization capability.

Adding Shared Drives in TL8, TLD, or TLH Robots

The wizard will configure shared drives on all of the media servers in your configuration that you select (see the wizard screen “Device Hosts” on page 39). Be sure to include the media server where the robotics are attached, so device serialization can be utilized.

The wizard adds `DEVICE_HOST` entries in the Media Manager `vm.conf` configuration file (see the wizard screen “Updating Device Configuration” on page 40).

Drives that are discovered by the wizard as cabled to the hosts that you selected are configured as shared drives. Robotic control is assigned to the first media server that scans for devices and discovers the robot.

Adding Shared Standalone Drives

Any standalone drives that are seen by the wizard as cabled to multiple hosts are configured as shared standalone drives.

All hosts that share the drive must use the same name for the drive. The wizard assigns these drive names.

The wizard also defines a common volume database host for the drives (by default, this is the master server).

Wizard Limitations

- You can use this wizard to configure devices only on the types of media servers shown in the following table. Auto-discovery used by the wizard depends on the existence of a way to issue SCSI pass-thru commands to the devices. The following table lists requirements for these media servers:

Server Type	Requirements
Windows	A tape driver must exist for each tape device.
Compaq Tru64 UNIX	Device files must exist following the naming conventions described in the Media Manager device configuration guide.
Sun Solaris	The sg driver must be properly configured and device files must exist following the naming conventions described in the Media Manager device configuration guide.
HP HP9000 HP-UX	Device files must exist following the naming conventions described in the Media Manager device configuration guide. Some HP SCSI adapters do not support SCSI pass-thru, so devices on these adapters are not auto-discovered.
IBM RS6000 AIX	The ovpass driver must be properly configured and device files must exist following the naming conventions described in the Media Manager device configuration guide.
SGI IRIX	Device files must exist following the naming conventions described in the Media Manager device configuration guide.

- To scan and auto-configure a device, all of the device hosts (media servers) that you select must be running the same NetBackup release (release 3.4 or later). The scan for devices will fail on hosts that are running older release levels.
- When configuring for SSO, this wizard does not support ACS or TLM robot types. This wizard also does not support LMF or RSM robot types (these robot types are not supported for SSO).
- If tape drives are in use or offline, they cannot be discovered.
- Auto-configuration depends on device serialization (see “Device Serialization” on page 37). For devices to be fully configured by this wizard, the following must be true for your configuration:
  - Each robot and drive reports a unique serial number.

  - Each robot reports the serial number of each of the drives contained within the robot.

- All information required for full auto-configuration may not be available on some systems. In this case, the wizard will do as much as possible with the limited device information. Later you need to manually configure the remaining devices (see "Completing Your Configuration" on page 44).
- After adding or removing devices from a SCSI bus, the operating system must be made aware of the new configuration before auto-discovery can be used. Often this requires a reboot of the operating system.

What To Expect In This Wizard

Wizard Screen	What to Expect
Welcome	You should have all required hardware and operating system configuration completed before starting the wizard (see "How To Get SSO Installed and Running" on page 5). The wizard does not do any of these tasks.
Device Hosts	You build (by adding hosts) the device host (or media server) list that the wizard uses to scan for devices. Be sure to include the host where the robotics are attached. You can change the order and contents of the list by adding or deleting hosts. Media Manager will record the shared device configuration on each host that you select in the device host list. The first host on the list that you select is scanned. This host becomes the robot control host if a robot is found on the SAN.

Wizard Screen	What to Expect
Scanning Hosts	All hosts that you selected in the previous screen are scanned. **Note** You may see a conflict error if the hosts you selected to scan do not agree as to which host stores global device information. For device discovery and auto-configuration to work properly, particularly where peripherals are connected to many servers, a single host must serve as the repository for global device configuration information. When you install NetBackup, this host is set by default to be the master server. However if you have multiple master servers, or did not install or upgrade your master servers before the media servers, then more than one host has been designated as the global device database host. Before continuing in the wizard, you need to specify a single host that will contain global device configuration information. VERITAS suggests that you specify your master server or one of the master servers, if you have several. You can select one of the hosts detected by the wizard (use the browse button in the dialog box) or you can enter another host name. Devices discovered by the scan are saved. If you cancel the wizard after this step, the wizard will roll back your configuration to the original settings.
Backup Devices	A list of the devices discovered by the wizard is presented for you to verify.
Drag and Drop Configuration	A device tree is presented that allows you to fine tune your configuration if needed, by dragging and dropping drives. See “Completing Your Configuration” on page 44.
Updating Device Configuration	Any drag and drop configuration changes are saved (`DEVICE_HOST` entries are placed in `vm.conf`), the Media Manager daemons/services are restarted, and a progress report is presented.
Configure Storage Units	A storage unit is created for each media server and this storage unit information is saved. This screen is skipped if all storage units are already configured.
Completion	A reminder appears that you can use the Media and Device Management interface to view and modify your configuration.

Running the Wizard for the First Time

The list of device hosts displayed will be empty, unless you have configured devices using the Media and Device Management interface (using the Add Robot and Add Drive dialogs). In this case, to perform a complete scan of your environment you should do the following in the Device Hosts screen of the wizard:

1. Click the **Add** button to add any device hosts with devices configured.

2. Check each box next to those device hosts.

Running the Wizard to Update Your Configuration

If you have added or moved devices on some device hosts in your configuration, you need only select those hosts in the device host list (see the wizard screen “Device Hosts” on page 39).

Note You can select all device hosts in your configuration. To have the wizard execute faster, select only the hosts affected by your changes.

After Adding a Drive

If you added a drive to a robotic library, select the device hosts where that drive is attached and also select the device host that has the robot control.

After Moving a Drive

If you moved a drive from device host A to host B, you need to select the following:

- Device host A.
- The device host that has the robot control (if applicable).
- Device host B.

Because of this move, each of these host’s configurations has changed and they must be rescanned by the wizard to accurately reflect this change and complete your configuration.

After Moving Robot Control

There is only one robot control host for each robot (except for ACS and TLM robot types). If you move the robot control from device host A to device host B, you need to select the following:

- Device host A.
- Device host B.

Because of this move, these host's configurations have changed and they must be rescanned by the wizard to accurately reflect this change and complete your configuration.

Running the Wizard More Than Once

If you are running the wizard to update your configuration, the list of device hosts shown in the Device Hosts screen of the wizard (see "Device Hosts" on page 39) matches the list that appears under the **Hosts** node of the NetBackup **Media and Device Management** window.

The list of device hosts displayed is a combination of device hosts that were added in any of the following ways:

- In previous executions of the wizard.
- Using the **Media and Device Management** interface.
- Manually to the Media Manager `vm.conf` configuration file.

To Start This Wizard

The Device Configuration wizard is available from the list of wizards displayed in the right pane of the **Media and Device Management** window of the NetBackup Administration Console.

Click **Media and Device Management** > **Configure Storage Devices**.

Configuration Problems With Devices That Do Not Support Serialization

If a robot or drive does not fully support device serialization, it is usually not possible for the wizard to completely configure the device. The greater the number of drives and robots in your configuration that do not support serialization, the greater the chance of having configuration problems using this wizard.

Robot or Drive Does Not Return A Serial Number

Suppose you have a robot that can contain two drives, but you initially install only one drive. Although the drive does not return a serial number the wizard is able to complete your configuration, because of the simplicity of the configuration.

Later, you install a second drive in the robot and run the wizard again. The wizard now discovers two drives in your configuration. Because these drives do not return serial numbers, the wizard cannot correctly configure the devices. The wizard is unable to determine which of the following is true:

- You added a new drive and kept the drive you originally configured.
- You added two new drives and removed the drive you originally configured.

Robot Does Not Return Serial Numbers For Each of Its Drives

If the robot does not return serial numbers for its drives, the wizard cannot determine which robot drive number should be assigned to the drives in the robot. This means that the wizard is unable to determine the order of the drives (their location) within the robot.

Also if a request for drive serial numbers fails, the wizard cannot determine whether the drive is in a robot or is a standalone drive.

For example, suppose you have a robot containing one drive and you have one standalone drive of the exact same drive type. If the robot does not support serialization, the wizard is unable to determine which drive is in the robot and which is the standalone drive.

Robot Returns Only The Number of Drives In The Robot

You may have a simple configuration (for example, one robot and one drive) and the robot returns one as the number of drives in the robot, but no serial number for the drive.

In this example

- The wizard is able to configure the devices. Because of the simplicity of this configuration, the serial number for the drive is not needed.
- You will see No in the Serialized column of the Backup Devices screen indicating that the device does not support serialization.

Determining If You have Devices That Do Not Support Serialization

1. Display the Backup Devices screen of the wizard.
2. Select each robot or drive shown in the list.

   If the device does not support serialization, No appears in the Serialized column.

If You have Devices That Do Not Support Serialization

You may be able to use the following methods to configure these devices:

- Use the Drag and Drop screen of the wizard.

  See “Completing Your Configuration” on page 44.

- Use the Shared Drive wizard. This wizard does not rely on device serialization.

  See “Shared Drive Wizard” on page 45.

Completing Your Configuration

The Drag and Drop Configuration screen of the wizard depicts where robotic drives are located in robots. From this screen, you can enable or disable the use of robots or non-shared drives by clicking the check boxes.

Note You cannot enable or disable shared drives in this wizard.

If your storage devices do not fully support serialization, you can use this screen to complete your configuration. If you have devices that do not fully support serialization and this is the first time you have run the wizard, or you did not make any configuration changes when you ran the wizard previously, you will see the following results on this wizard screen:

- Any unconfigured drives for a robot appear under the Standalone Drives node.
- The robot node will have empty nodes under it for each available drive address in the robot.

If you have an unconfigured robot with drives, do the following in the Drag and Drop Configuration screen:

1. If you know the correct drive numbers in the robot, drag the drives to the empty drive node having the corresponding drive number in this robot.

   Refer to your vendor documentation for the robot or the Robot Drive and Slot Layout appendix in the NetBackup Media Manager system administrator’s guide for help in determining the drive numbers.

2. If you want the robot and drives enabled, select the check boxes for the robot and drives.

Shared Drive Wizard

This wizard configures shared drives in ACS or TLM robot types. You can also add shared standalone drives with this wizard.

You can use this wizard to configure shared drives in TL8, TLD, or TLH robot types, but the Device Configuration wizard (see “Adding Shared Drives in TL8, TLD, or TLH Robots” on page 37) is recommended for these types.

What To Expect In This Wizard

Wizard Does Not Configure Robots

This wizard does not configure robots. To configure SSO for these robot types, you must

1. Configure robots using the Media Manager **Media and Device Management** interface.

   TLM robot types require an extra step. See “Configuring the DAS Server for TLM Robot Types” on page 48 for information.

2. Use the Shared Drive wizard to add shared drives.

Wizard Does Not Use Device Serialization

Since this wizard does not use device serialization, it requires more configuration details from you (see “Before You Start This Wizard”). The configuration information prompted by the wizard varies depending on whether you are

- Adding a new shared drive.

  See “Adding Shared Drives in ACS or TLM Robots” on page 47.

- Adding a shared drive by reconfiguring an existing drive. In this case, you specify a host that is currently sharing this drive.

  See “Adding Shared Drives in ACS or TLM Robots” on page 47.

- Changing the configuration for an existing shared drive.

  See “Changing an Existing Shared Drive in ACS or TLM Robots” on page 47.

At the End of the Wizard

Your configuration changes are saved. At this point you can choose to

- Run the configuration analyzer (see "Media and Device Management Configuration Analyzer" on page 67).
- Restart the Media Manager daemons / services on all device hosts that share the drive.

Before You Start This Wizard

Obtain and note the following information for your configuration, so that you can accurately respond to the wizard prompts:

- The name for the drive. This name *must* be the same across all hosts that will share the drive and should be descriptive. If the logical names of the drives are not consistent across all hosts, you will receive the following:
  - Error messages when you run the configuration analyzer to display configuration conflicts (see "Media and Device Management Configuration Analyzer" on page 67).
  - Drive reservation conflicts which may cause downed drives.

  The drive name must also *remain* the same if you later change the attributes of the drive (see "Changing an Existing Shared Drive in ACS or TLM Robots" on page 47).
- The type of the drive.
- The robotic drive parameters and the number of the robot that will control the drive, if the drive is in a robotic library.
  - If the robot type is ACS, you specify four numbers for the drive.
  - If the robot type is TLM, you specify the DAS drive name.

  Except for ACS and TLM robot types, there is only one robot control host for each robot and you specify the host where the robot control is configured.
- The name of the volume database host for the drive, if the drive is a standalone drive. This host should be the same volume database host as for *all* other standalone drives.

Caution If the volume database host for the standalone drive is *not* the same volume database host as for all other standalone drives, serious configuration problems can occur (see "Volume Database Host (Device Allocation Host)" on page 30).

- The names of the hosts that will share this drive. Remember that *each* host that shares the drive must have a license for SSO.
- If you add additional hosts that will share the drive, you need to know the drive path for each host. On Windows hosts, the drive path is the name of the drive as it is recognized by operating system. On UNIX hosts, the drive path is the name of the no rewind on close device file.

Check your notes to ensure that you are assigning the correct robot drive address to each drive path.

- When adding drives in a mixed environment (UNIX and Windows hosts), confirm the device names on each of the hosts before defining the drives on the master server.

Adding Shared Drives in ACS or TLM Robots

Wizard Capabilities

The shared drive wizard does not configure robots. You must first configure the robot using the **Media and Device Management Devices** interface (see "What To Expect In This Wizard" on page 45).

To configure a shared drive with this wizard, you can do either of the following:

- Add a new shared drive.
- Reconfigure an existing non-shared drive to be a shared drive.

  You can change the attributes of the existing drive or leave the attributes unchanged.

To Start The Wizard

This wizard is available from the list of wizards displayed in the right pane of the **Media and Device Management** window of the NetBackup Administration Console.

Click **Media and Device Management** > **Configure a Shared Drive**.

You can also start this wizard using the following alternate procedure:

1. In NetBackup Administration Console, click **Media and Device Management** > **Devices**.
2. Click **Actions** > **New** > **Shared Drive**.

This starts a wizard that guides you through the steps involved in configuring shared drives.

Changing an Existing Shared Drive in ACS or TLM Robots

Wizard Capabilities

You can do either of the following types of changes:

- Share the drive with additional hosts or change the drive path for a host.
- Change the current attributes of the shared drive.

To Start the Wizard

1. In NetBackup Administration Console, click **Media and Device Management** > **Devices**.
2. Select the **Drives** tab in the Devices pane.
3. Select the shared drive you want to change.
4. Right-click and select **Configure Shared Drive** on the shortcut menu.

The wizard is started and guides you through the steps involved in changing the configuration for the shared drive.

Configuring the DAS Server for TLM Robot Types

Using TLM robots with SSO requires that the ADIC DAS server be configured to allow drives to be allocated in DAS simultaneously to all hosts sharing the drives. For more information see the TLM appendix of the NetBackup Media Manager system administrator's guide.

Using the Volume Configuration Wizard to Configure Media

Run the Volume Configuration wizard to

- Inventory your robots.
- Add volumes for standalone drives.
- Update the Media Manager volume database.

After running this wizard to configure media, each media will have a unique media ID in the volume database that is used in Media Manager and NetBackup to track the media.

Wizard Limitations

This wizard is only available in NetBackup release 3.4 or later releases.

This wizard configures volumes for standalone drives and robots, but *does not* support the configuring of volumes for the following devices:

- Robots that have more than one type of drive.

  A robot is considered to have more than one type of drive if the media written in any one drive cannot be read and written in every other drive. This includes drives that are different versions of the same family of drives. For example, a robot with a Quantum DLT7000 drive and a Quantum DLT8000 drive is considered to have different drive types.

- API robots.

  API robots that are applicable to SSO are ACS, TLH, and TLM Media Manager robot types. These robots manage their own media.

- Optical robots and optical standalone drives.

To configure volumes for these devices, you must use the robot inventory of the Media and Device Management administrative interface.

What To Expect In This Wizard

Wizard Screen	What to Expect
Welcome	With this wizard you can - Inventory the volumes in a robot. - Create new volumes for use in standalone drives.
Select Device	You select one of the following: - The robot that you want to inventory. - The type of standalone drive where you want to configure volumes. Robots that have more than one type of drive are not supported (see "Wizard Limitations" on page 48). In some cases the wizard is unable to determine if more than one type of drive exists in the robot. In this case, you must specify whether or not the robot has multiple drive types.
Robot Inventory (*Only if a robot was selected*)	You start the inventory which updates the Media Manager volume database.
Robot Inventory (*Only if a robot was selected*)	You can view the results of the inventory.

Wizard Screen	What to Expect
Identify Cleaning Media (*Only if a robot was selected*)	To avoid any potential problems in the Media Manager volume database, you select the slots in the robot that are known to contain cleaning media.
Volumes for Standalone Drives (*Only if a standalone drive was selected*)	You specify the number of volumes to configure for the selected drive type. The Media Manager volume database is updated when you click **Next**.
Completion	You can choose to go back and configure more volumes if necessary, or exit the wizard.

Before You Start This Wizard

Make sure that you have all media that you want to use for SSO testing in the robot before starting the wizard.

To Start This Wizard

This wizard is available from the list of wizards displayed in the right pane of the **Media and Device Management** window of the NetBackup Administration Console.

Click **Media and Device Management** > **Configure Volumes**.

Using Alternate Interfaces for SSO Device Configuration

There are alternatives available for configuring shared drives but they do not include important diagnostic tools, such as the following:

- Device management reports (see “Media and Device Management Summary Reports” on page 67).
- Configuration analysis (see “Media and Device Management Configuration Analyzer” on page 67).

These configuration alternatives require manual configuration instead of using automated methods like device serialization and have an increased chance for configuration errors.

Note Using the Media Manager wizards is recommended.

tpconfig menus (UNIX)

If you use this interface, make sure that

- All hosts that are sharing the drive use the same case-sensitive name for the drive (descriptive names are recommended).
- You define a common volume database host.

For more information about using this utility, see the appendix of the UNIX NetBackup Media Manager system administrator's guide.

tpconfig Command Line Interface (UNIX or Windows)

If you use this CLI interface, use the `-shared yes` option with the `-add -drive` or `-update -drive` commands when defining shared drives.

For more information, see `tpconfig` in the appendix of the NetBackup Media Manager system administrator's guide.

Verifying Your SSO Configuration 6

In some SSO configurations, such as those involving fibre channel-attached tape drives, it is difficult to determine the logical device name for a physical tape drive without performing I/O through the tape device.

Use the following resources when multiple hosts are sharing drives in a robotic tape library:

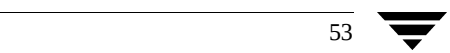
- Use the SSO information and tools that are available from Media Manager to check your configuration. See "Viewing SSO Configuration Information" on page 65.
- Use the `robtest` test utility and the Device Monitor administrator interface to verify that each server can access all shared drives and the robots.
- After attempting to correlate the physical drive addressing (SCSI targets) with information from device scans or as a configuration check, use one of the following verification procedures (depending on the type of your host platform) to verify your device configuration.

Note The `vmdareq` command shown in these procedures should be used for diagnostic purposes only. The options and the output of this command may change in future releases of NetBackup.

Verifying Your Configuration On Windows Hosts

1. From the NetBackup Administration Console, click **Devices** > **Actions** > **Stop/Restart Device Manager Service** to start the device manager service (`ltid`) on the host with the robotic control. For TL8, TLD, and TLH robot types, there is only one robot control host for each robot. In configurations with only ACS or TLM robots, start `ltid` on one of the hosts that shares the drives.

   In this procedure, this host is identified as *host1*. Ensure that the NetBackup Volume Manager service is running on all hosts, since it is needed for remote configuration. This service is normally started when you start the NetBackup Device Manager service. You can control the NetBackup Device Manager service using **Actions** > **Stop/Restart Device Manager Service**.



2. Identify the device allocation host where vmd/DA is running (see "vmd/DA" on page 89). This is the host that is serving as the volume database host for the robot with shared drives (see "Device Allocation Host" on page 92).

   (When multiple robots or standalone drives are involved, there may be more than one DA host, but each physical drive must be allocated from only one DA host.)

3. Obtain the current device allocation state by sending the following command to the DA host(s):

   install_path\volmgr\bin\vmdareq -h *DA-Host* -display

   For example,

   install_path\volmgr\bin\vmdareq -h host1 -display

   Results in the following:

   ```
   drive1 - AVAILABLE
   host1 SCAN_HOST
   drive2 - AVAILABLE
   host1 SCAN_HOST
   ```

   This display indicates that drive1 and drive2 have registered with the DA host. There is only one host (host1) registered with the DA host and it has been assigned the role of scanning the drives (as indicated by the SCAN_HOST identifier). host1 lines appear twice because this host is scanning drive1 and drive2.

Note If applicable, you can also use the Shared Drive Summary report available in the UNIX Device Monitor (see "Media and Device Management Summary Reports" on page 67).

4. If there are no hosts listed, start the NetBackup Device Manager service on *host1*, so that the host registers with vmd/DA. If there is more than one host registered for a shared drive, stop the service on all hosts that are not *host1*. Stop all services and reissue the vmdareq command until only one host is registered.

   If *host1* has the robotic control but no drives attached, start the NetBackup Device Manager service on another host that is sharing the drive. Consider this host to be *host1* in the following steps.

5. Start the **Device Monitor** (see "Drive Status List of the Device Monitor" on page 65) and select *host1* as the device host. Verify that the shared drives are up, and that the control column for robotic drives shows the robot type (for example, TLD).

   If it does not show this state, there is a hardware problem or configuration error. Stop using this procedure and investigate the device configuration and the system application log to help resolve the problem. If the control column shows the robot type for the robotic shared drives, proceed to the next step.

6. Use the robotic test utility (*install_path*\volmgr\bin\robtest) to mount a tape on one of the drives to verify that each host can "see" the drive.

Caution The automated robotic processes controlling the robot may be disabled while robtest is active. Make sure you exit the robtest to avoid problems.

7. Use the **Device Monitor** to verify that the tape was mounted on the correct drive, for example, the drive that was specified in robtest. Since *host1* is the scan host (see "Scan Host" on page 91), when a drive becomes ready after a tape is loaded, you can determine which device name is associated with the targeted drive. If the correct drive did not become ready, reconfigure the drives on *host1* and stop and restart the NetBackup Device Manager service so that the device name is associated with the correct drive.

Note If you restart the NetBackup Device Manager service on the host that is currently the scan host, another host will become the new scan host (if its NetBackup Device Manager service is running).

8. Unload the drive using the SCSI unload command found in the robotic test utility, if *host1* has robotic control. Otherwise, use the drive's manual unload button or a toolkit.

   Use robtest to move the tape volume into the next drive, and repeat the verification step of observing the results in the Device Monitor display.

9. When all drive paths on *host1* have been verified, start the NetBackup Device Manager service on a second host, *host2*. Verify that *host2* correctly registers its shared drives with vmd/DA using the following command:

   install_path\volmgr\bin\vmdareq -h host1 -display

   This results in the following:

```
drive1 - AVAILABLE
host1 SCAN_HOST
host2
drive2 - AVAILABLE
host1 SCAN_HOST
host2
```

   This display indicates that drive1 and drive2 have registered with the DA host. There are two hosts (host1 and host2) now registered with the DA host. host1 is still assigned the role of scanning the drives (as indicated by the SCAN_HOST identifier). host1 and host2 lines appear below each drive, because both hosts are scanning both drives.

10. Send the following command to vmd/DA to allow *host2* to take over the drive scanning. *host1* will become available after a short amount of time, but this command forces *host2* to become the new scan host.

install_path\volmgr\bin\vmdareq -h *DA-Host* -unavailable -H host1

11. Reissue the command to see that the scanning responsibility has shifted to *host2*:

```
vmdareq -h host1 -display
```

This results in the following:

```
drive1 - AVAILABLE
host1 UNAVAILABLE
host2 SCAN_HOST
drive2 - AVAILABLE
host1 UNAVAILABLE
host2 SCAN_HOST
```

This display indicates that host2 is assigned the role of scanning the drives (indicated by the SCAN_HOST identifier). The UNAVAILABLE identifier for host1 is temporary.

12. Change the Device Monitor device host to *host2*. On *host1* which has the robotic control, use robtest to mount a volume in a drive. Verify the correct drive address using the Device Monitor.

Unload the drive on *host2*.You may need to use the manual unload button, or stop the NetBackup Device Manager service on *host2* and unload using robtest on *host1*.

This will verify all device names on *host2*.

13. Start the NetBackup Device Manager service on the third host, if more than two hosts are sharing drives. Stop the service on *host2*. Use vmdareq to verify that *host3* is now the scan host for its shared drives.

host1 may become available again after a period of time. If *host1* is the scan host, perform step 10 to allow *host3* to become the scan host.

14. Repeat step 12 to verify the *host3* device names.

Repeat this complete procedure until device names have been verified on all hosts. Stop and restart the NetBackup Device Manager service on *host1* and start it on all other hosts.

15. Verify the following with vmdareq:

- All hosts are registered with vmd/DA.
- There are no unavailable hosts.

- Each shared drive has a designated scan host.

Verifying Your Configuration On UNIX Hosts

1. From the NetBackup Administration Console, click **Devices** > **Actions** > **Stop/Restart Device Manager Service** to start the Media Manager device daemon (`ltid`) on the host with the robotic control. For TL8, TLD, and TLH robot types, there is only one robot control host for each robot. In configurations with only ACS or TLM robots, start `ltid` on one of the hosts that shares the drives.

   In this procedure, this host is identified as *host1*. Ensure that the Media Manager volume daemon (`vmd`) is running on all hosts, since it is needed for remote configuration. The volume daemon is normally started when you start the device daemon. You can control the Media Manager device daemon using **Actions** > **Stop/Restart Media Manager Device Daemon**.

2. Identify the device allocation host where `vmd/DA` is running (see "vmd/DA" on page 89). This is the host that is serving as the volume database host for the robot with shared drives (see "Device Allocation Host" on page 92).

   (When multiple robots or standalone drives are involved, there may be more than one DA host, but each physical drive must be allocated from only one DA host.)

3. Obtain the current device allocation state by sending the following command to the DA host(s):

   `/usr/openv/volmgr/bin/vmdareq -h` *DA-Host* `-display`

   For example,

   `/usr/openv/volmgr/bin/vmdareq -h host1 -display`

   Results in the following:

   ```
   drive1 - AVAILABLE
   host1 SCAN_HOST
   drive2 - AVAILABLE
   host1 SCAN_HOST
   ```

   This display indicates that `drive1` and `drive2` have registered with the DA host. There is only one host (`host1`) registered with the DA host and it has been assigned the role of scanning the drives (as indicated by the `SCAN_HOST` identifier). `host1` lines appear twice because this host is scanning `drive1` and `drive2`.

Note You can also use the Shared Drive Summary report available in the UNIX Device Monitor (see "Media and Device Management Summary Reports" on page 67).

4. If there are no hosts listed, start the device daemon on *host1*, so that the host registers with `vmd/DA`. If there is more than one host registered for a shared drive, stop the daemon on all hosts that are not *host1*. Stop the device daemons and reissue the `vmdareq` command until only one host is registered.

5. Start the **Device Monitor** (see "Drive Status List of the Device Monitor" on page 65) and select *host1* as the device host. Verify that the shared drives are up and that the control column for robotic drives shows the robot type (for example, TLD).

   If it does not show this state, there is a hardware problem or configuration error. Stop using this procedure and investigate the device configuration and the system application log to help resolve the problem. If the control column shows the robot type for the robotic shared drives, proceed to the next step.

6. Use the robotic test utility (`/usr/openv/volmgr/robtest`) to mount a tape on one of the drives.

Caution The automated robotic processes controlling the robot may be disabled while `robtest` is active. Make sure you exit the robtest to avoid problems.

7. Use the Device Monitor to verify that the tape was mounted on the correct drive, for example, the drive that was specified in `robtest`. Since *host1* is the scan host (see "Scan Host" on page 91), when a drive becomes ready after a tape is loaded, you can determine which drive path is associated with the targeted drive. If the correct drive did not become ready, reconfigure the drives on *host1* and stop and restart the device daemon so that the drive path is associated with the correct drive.

Note If you restart the device daemon on the host that is currently the scan host, another host will become the new scan host (if its device daemon is running).

8. Unload the drive using the SCSI unload command found in the robotic test utility, if *host1* has robotic control. Otherwise, use the drive's manual unload button or a toolkit.

   Use `robtest` to move the tape volume into the next drive, and repeat the verification step of observing the results in the Device Monitor display.

9. When all drive paths on *host1* have been verified, start the device daemon on a second host, *host2*. Verify that *host2* correctly registers its shared drives with `vmd/DA` using the following command:

   ```
   /usr/openv/volmgr/bin/vmdareq -h host1 -display
   ```

   This results in the following:

   ```
   drive1 - AVAILABLE
   ```

```
host1 SCAN_HOST
host2
drive2 - AVAILABLE
host1 SCAN_HOST
host2
```

This display indicates that drive1 and drive2 have registered with the DA host. There are two hosts (host1 and host2) now registered with the DA host. host1 is still assigned the role of scanning the drives (as indicated by the SCAN_HOST identifier). host1 and host2 lines appear below each drive, because both hosts are scanning both drives.

10. Send the following command to vmd/DA to allow *host2* to take over the drive scanning. *host1* will become available after a short amount of time, but this command forces *host2* to become the new scan host.

```
/usr/openv/volmgr/bin/vmdareq -h DA-Host -unavailable -H host1
```

11. Reissue the command to see that the scanning responsibility has shifted to *host2*:

```
vmdareq -h host1 -display
```

This results in the following:

```
drive1 - AVAILABLE
host1 UNAVAILABLE
host2 SCAN_HOST
drive2 - AVAILABLE
host1 UNAVAILABLE
host2 SCAN_HOST
```

This display indicates that host2 is assigned the role of scanning the drives (as indicated by the SCAN_HOST identifier). The UNAVAILABLE identifier for host1 is temporary.

12. Change the Device Monitor device host to *host2*. On *host1* which has the robotic control, use robtest to mount a volume in a drive. Verify the correct drive address using the Device Monitor.

Unload the drive on *host2*.You may need to use the manual unload button, or stop the NetBackup Device Manager service on *host2* and unload using robtest on *host1*.

This will verify all device names on *host2*.

13. Start the device daemon on the third host, if more than two hosts are sharing drives. Stop the device daemon on *host2*. Use vmdareq to verify that *host3* is now the scan host for its shared drives.

host1 may become available again after a period of time. If *host1* is the scan host, perform step 10 to allow *host3* to become the scan host.

14. Repeat step 12 to verify the *host3* drive paths.

    Repeat this complete procedure until the drive paths have been verified on all hosts. Stop and restart the device daemon on *host1* and start it on all other hosts.

15. Verify the following with `vmdareq`:

    - All hosts are registered with `vmd/DA`.
    - There are no unavailable hosts.
    - Each shared drive has a designated scan host.

Configuring SSO Usage in NetBackup 7

This chapter explains what you need to do in the **Storage Units** and **Policies** nodes of the NetBackup Administration Console to use SSO.

See the NetBackup system administrator's guide for more detailed information.

Configuring Storage Units and Backup Policies

On the master server, configure storage units and policies for your shared drives. If the device configuration wizard was used, storage units may have already been configured by the wizard (see "What To Expect In This Wizard" on page 39).

Configuring Storage Units for Each Media Server

In each storage unit definition, you logically define the robot and the shared drives for that media server. For the number of drives used for backup (**Maximum concurrent drives used for backup**), you should specify the total number of all shared drives in the robot.

For example, suppose you have a configuration with four servers (dog1, pony2, frog3, and fish4) sharing six drives in one robot. The server dog1 is the master server and is the robot control host for the robot that contains the six drives that are being shared.

You would configure a storage unit on master server dog1 for the robot and specify six as the maximum concurrent drives used for backup. Also on the server dog1, you would configure a storage unit for the robot and specify six for the number of concurrent drives, for the following:

- Server pony2
- Server frog3
- Server fish4

Reserving a Drive for Restore Jobs

If you want to reserve a drive for all servers to share for restores, you would specify one less than the total number of shared drives available for the number of drives.

Configuring A Backup Policy for Each Media Server

VERITAS licenses a *regular media server* that can back up its own data or other network clients as well. VERITAS also licenses a *SAN media server* that can only back up its own data to shared drives—no backing up of data resident on other clients is allowed.

A license for a regular media server provides the greatest flexibility in configuring policies. A license for a SAN media server is more restrictive, but is less costly.

Defining a policy for a media server depends on your VERITAS license, as follows:

- If you are defining a policy for a regular media server that is using SSO, then the policy can contain the media server (itself) as a client and any other network clients that you want to back up across the SAN to this media server.
- If you are defining a policy for a SAN media server, then the policy will have just one client—the SAN media server—and will use the specific storage unit.

If you are defining a policy for network clients that you want to back up anywhere in your configuration, you can list all of the clients and choose **Any_available** (on NetBackup UNIX servers) or **Any available** (on NetBackup Windows servers) as the policy storage unit or use the storage unit groups (prioritized storage units).

Directing a Media Server To Use Its Own Drives

Backups normally are run on any server that has drive capacity available. This can be an issue in SSO SAN environments where backup jobs that could be done locally, are sent across the LAN to another available drive, thus reducing backup performance.

If you want to configure a media server to back up its own data over the SAN to its own shared drives (local), rather than across the LAN to another media server with an available drive, see the following topics in this section. These configurations will probably provide quicker access to the shared drive, even when considering any possible wait time for the drive to become available.

The `MUST_USE_LOCAL_DRIVE` parameter was introduced to make directing a server to use its own drives much easier. By adding this option, a backup of a SAN media server (see “Configuring A Backup Policy for Each Media Server” on page 62) will send the data over the SAN to a local drive.

Depending on the type of your server, specify this parameter in the NetBackup `bp.conf` configuration file on UNIX servers or in the Windows registry by using the configuration utility. `MUST_USE_LOCAL_DRIVE` can also be found in the NetBackup Administration Console (**Host Properties** > **Master Server** > **General** tab).

This parameter allows the use of any available as the policy storage unit and removes the need to define a policy for each media server that calls for the specific storage unit for that media server. You still need to configure a storage unit for each media server.

You can mix clients in a policy, use any available, and when the backup starts for the client that is a SAN media server, the backups will be directed to the SAN connected drives on that server.

If a client is not a server, this parameter has no effect.

If you use this parameter and the local drives are all down or busy, any subsequent jobs will be queued. If all of the drives become unavailable, you will have to remove the storage unit or remove the parameter.

Drive Allocation Problems

If a media server has *both* shared and non-shared drives, *do not* do either of the following actions. These actions can result in drive allocation problems.

- Specify `MUST_USE_LOCAL_DRIVE` in the `bp.conf` file on that media server.
- Configure any policy to use only a specific storage unit that is on that media server.

Duplication Jobs

The NetBackup scheduler is aware of duplication jobs and will not overcommit jobs if drives are being used for duplication and no drives are available. Drives are only allocated to a particular media server while a job is active. As soon as the job finishes, the drive is released and made available to any other media server that is sharing the drives.

Using SSO 8

This chapter explains how to

- Obtain information about your SSO configuration in Media Manager.
- Fine tune your configuration by using SSO options in the Media Manager configuration file.
- Improve performance when using SSO.

Viewing SSO Configuration Information

The Device Monitor window of the NetBackup Administration Console provides the following SSO configuration information.

Drive Status List of the Device Monitor

The following columns in the Drive Status list are of note when using SSO. The Drive Status list is displayed in the upper pane of the Device Monitor window. See the Media Manager system administrator's guide for more information.

Column	Contents
Assigned Host	This column shows the device host that currently has the drive assigned. If the selected drive is not assigned, this column is blank.
Shared	If the selected drive is configured as a shared drive, this column contains Yes. If the drive is not a shared drive, the column contains No.

Column	Contents
Control	Control mode for the drive. Control mode can be any of the following: - *robot_designation.* For drives in a robot. For example, TLD. - DOWN-*robot_designation.* For drives in a robot. For example, DOWN-TLD. - DOWN. For standalone drives only. In this mode, the drive is not available to Media Manager. A drive can be in a DOWN mode because of problems or because it was set to that mode using **Actions** > **Down Drive**. - PEND-*robot_designation*. For drives in a robot. For example, PEND-TLD. - PEND. For standalone drives only. If the drive reports a SCSI RESERVATION CONFLICT status, this column will show PEND. This status means that the drive is reserved when it should not be. Several operating systems (Windows, Tru64, and HP-UX) also may report PEND if the drive reports Busy when opened. This reporting is likely caused by errors in the configuration. See "SCSI Reserve / Release" on page 71 for details. - AVR (up in Automatic Volume Recognition mode). For standalone drives only. This is the normal operating mode. - OPR (up in operator control mode). For standalone drives only. - <Mixed> The control modes of the shared drives are not all the same. If the control modes *are* all the same, that mode is displayed. If the drive is a shared drive, click **Actions** > **Drive Details** to view the drive control mode for each host that is sharing this drive.

Media and Device Management Summary Reports

These reports are available from the Device Monitor in the NetBackup Administration Console *only* on UNIX servers.

The reports contain Media Manager information about your SSO configuration (see "SSO Components in Media Manager" on page 88).

Report	SSO Information
Shared Drive Summary	Drive name, device allocation host, the number of registered hosts, drive reservation status, reserved hosts, and the scan host.
Device Allocation Host Summary	The device allocation host, host name of the registered host, the number of registered and reserved drives, availability status, the scan ability factor, and scanning status.

To View These Reports

1. In NetBackup Administration Console, click **Media and Device Management** > **Device Monitor**.
2. Click **Actions** > **View Shared Drive Status** to display a dialog box that allows you to display these reports.
3. Select a device allocation host (or hosts) from the list and use **Add >>** to move it to the list of hosts that will be scanned.
4. Click **OK**. The reports appear in the two lower panes.

Media and Device Management Configuration Analyzer

SSO naming and configuration conflicts can be checked with the configuration analyzer. The analyzer verifies that the settings in your SSO configuration are consistent and checks for potential configuration problems.

The analyzer may produce informational (INFO), warning (WARN), and error (ERR) categories of messages.

The analyzer checks

- Communication links with `vmd` and `ltid` on all known hosts.

  The analyzer will report if `vmd` and `ltid` are inactive. On some hosts, `ltid` can be inactive. `ltid` needs to be running if a drive is configured on the host.

- Robotic parameters (including robot number, robot type, and robot drive number).
- If robot numbers are being reused.

  All robots in your SSO configuration should have unique numbers. This makes identification easier and may avoid a loss of data.
- For duplicate robotic definitions (robot control should be on only one host).
- For inconsistent robotic paths.
- If a drive is configured as both shared and non-shared.
- For drive conflicts, such as, hosts having drive information containing different attributes for the same shared drive.

  For example, one host may see a shared drive's type as DLT cartridge and another host may see the type configured as 1/2 inch cartridge.
- If a shared drive has different robot drive numbers.

To View This Report

This report is available from the Device Monitor in the NetBackup Administration Console on UNIX servers and from the Shared Drive wizard (see "Shared Drive Wizard" on page 45).

You can start the analyzer in either of the following ways:

- From the Device Monitor, click **Actions** > **Analyze Device Configuration**.
- From the final screen of the Shared Drive Wizard, you can choose to start the analyzer after your configuration changes are saved.

In the configuration analyzer, select a drive and the hosts that share this drive that you want to check.

SSO Configuration Options for the vm.conf File

The following optional entries for shared drives can be added to the Media Manager `vm.conf` configuration file on any media server.

See "SSO Components in Media Manager" on page 88 for information on the SSO terms used in the following descriptions.

See the Media Manager reference topics appendix in the Media Manager system administrator's guide for descriptions of all of the available `vm.conf` entries.

SSO Host Name

`SSO_HOST_NAME =` *host_name*

Specifies the name used by the current host to register, reserve, and release shared drives with `vmd/DA`. The default is the local host name.

Scan Ability Factor

`SSO_SCAN_ABILITY =` *factor*

factor can be an integer from 1 to 9, and has a default value of 5.

When `ltid` registers with `vmd/DA` it specifies a scan ability factor. This factor allows the assignment of scan hosts to be prioritized if a drive's scan host changes.

For example, if a host is underpowered and you do not want to use it as a scan host, you could add the following configuration entry on that host:

```
SSO_SCAN_ABILITY = 1
```

Then if the scan host for a drive is changed and there are other available hosts (registered for that drive) that have a higher scan ability factor, they will be chosen first. Likewise, a high-powered server may have a scan ability of 9 assigned and will be chosen as the new scan host (over other hosts that have a scan ability of less than 9) whenever the scan host changes. The host that has the role of scan host would change for example, if the current host was placed offline for repairs.

Device Allocator Retry Timeout

If `ltid` on a host in a shared drive configuration encounters problems during communications with `vmd/DA` or a failure while attempting to reserve a shared drive with `vmd/DA`, it delays before trying again.

You can tune this delay period by adding the following entry on the device host where `ltid` is running:

`SSO_DA_RETRY_TIMEOUT =` *delay_in_minutes*

delay_in_minutes can be an integer from 1 to *n*, and has a default value of 3.

For example:

```
SSO_DA_RETRY_TIMEOUT = 2
```

After adding this entry, `ltid` must be stopped and restarted for the change to take effect.

If you specify a low timeout value, the load on `vmd/DA` is increased. `vmd/DA` may not be able to satisfy all of its requests if many hosts request its services often. This is especially true when large or many volume-related requests (such as refreshes of volume information in media management interfaces) are active.

Device Allocator Reregister Interval

`ltid` on a scan host periodically re-registers its shared drives with `vmd/DA` to ensure that it is still providing the drive scanning function on behalf of other hosts. This allows conditions such as, a device allocator (`vmd/DA`) restart to have minimal impact on the use of shared drives.

By default, the re-registration interval is five minutes. You can tune this interval by adding the following entry on the host where `ltid` is running:

`SSO_DA_REREGISTER_INTERVAL =` *delay_in_minutes*

For example:

```
SSO_DA_REREGISTER_INTERVAL = 4
```

After adding this entry, `ltid` must be stopped and restarted for the change to take effect.

If you specify a short interval, the load on `vmd/DA` is increased. This load is not significant if there are few scan hosts or few shared drives managed by a particular `vmd/DA`.

Throughput Optimization

This is a NetBackup (data path) specific issue and deals with client disk read and write speeds, network speeds, and tape writing and reading speeds. Most of the "tuning knobs" are NetBackup specific, not Media Manager or SSO specific.

See the NetBackup system administrator's guide for more information on this topic.

SCSI Reserve/Release 9

This chapter includes the following topics to help you understand SCSI reserve / release in an SSO environment:

- "Background Topics"
- "How NetBackup Uses SCSI Reserve / Release Commands"
- "Issuing Reset Commands to Break a Reservation"
- "Controlling SCSI Reserve / Release"
- "SCSI Reserve / Release Requirements and Limitations"

Background Topics

The following topics explain a major change in the implementation of NetBackup SSO and an overview of the SCSI reserve / release functionality.

Releases Prior to NetBackup 4.5

In previous releases, Media Manager used a network protocol for drive reservations. Unfortunately in some situations, this allowed any program outside the local NetBackup realm to access drives without Netbackup being aware of the fact (this was true for drives in SSO and SAN configurations, and also for non-SSO locally attached drives).

In SAN configurations, NetBackup could have a drive open for read or write operations on one host and the device could be accessed by another host. This situation could occur since there was no single tape driver controlling access to the device. If an external program moved the tape for any reason during a Netbackup operation, data corruption could be the result, since NetBackup assumed the tape position was unchanged from the last command NetBackup had issued to the drive.

For NetBackup Release 4.5

In multiple-initiator (multiple HBA) environments (such as SSO configurations), some form of device level protection is required to avoid unintended sharing of tape devices and possible data loss problems. The only widely available technique for this purpose is to use SCSI reserve / release functionality.

Starting with release 4.5, NetBackup uses SCSI reserve / release commands to improve data integrity. SCSI reserve / release operates at the SCSI target level and depends on the fibre-to-scsi bridge or the native fibre device hardware working correctly.

SCSI Reserve/Release Commands

When a device receives a SCSI reserve command, it will no longer process commands from any other HBA until the reserving HBA issues the SCSI release command. If an application sends a command to a reserved device, the device will fail the command by returning a status of RESERVATION CONFLICT. The only exceptions to this action are the Inquiry, Log Sense, Report LUNs, and Request Sense commands, which will return the requested information.

A device stays reserved until one of the following actions occurs. The device is

- Released by the HBA that reserved it.
- Released by some sort of TARGET or LOGICAL UNIT RESET. These resets are protocol dependent, and differ between parallel SCSI and FCP (SCSI on fibre channel). These resets may be issued from any HBA.
- Power cycled.
- Released by fibre channel LOGO / PLOGO / PRLI / PRLO / TPRLO or failed discovery (link actions).

A negative effect of SCSI reserve can occur if the reserving HBA stops working (for example, due to a system crash or hardware failure). All devices reserved by the HBA stay reserved until the reservation is removed or broken. The reservation can only be removed by the original HBA, which means the system must be available. In the case of a hardware failure, this is not possible.

To break a reservation the device must be reset. This can be done by any of the following:

- SCSI reset
- Bus device reset
- LUN device reset
- Power cycle
- Fibre channel link actions may break reservations.

SCSI reserve and SCSI release commands are mandatory for all SCSI-2 and SCSI-3 devices. See the SCSI 2 standard for a detailed description of SCSI reserve command operation and behavior.

How NetBackup Uses SCSI Reserve/Release Commands

The following topics explain how NetBackup uses SCSI reserve / release commands in an SSO environment (or any other multiple-initiator environment). The same basic operations are done by other VERITAS applications (for example, VERITAS Storage Migrator components).

Issuing the Reserve

On DYNIX, HP-UX, IRIX, Solaris, AIX, TRU64, Linux, and Windows Servers

The NetBackup processes (`bptm`, `bprecover`, and `bpbackupdb`) that read or write tape media issue a SCSI reserve command to the tape device that contains the media in use (during the open process). Once the reservation is established, all other HBAs are locked out of this tape device. This reservation prevents other HBAs from issuing commands that can cause data loss.

This reservation *does not* prevent other applications from using the same device on the server with the reservation and causing data loss (for example, someone issuing a UNIX `mt` command).

Checking for Data Loss

On HP-UX, Solaris, AIX, TRU64, and Windows Servers

The `bptm` process detects data loss by reading the tape position and then checking the actual position against the expected position. If the actual position is less than the expected position (at the end of the backup process), the following will occur:

- The tape is frozen.
- The backup fails.
- The following error message entry is placed in the error log:

```
FREEZING media id xxxxxx, External event caused rewind during
write, all data on media is lost
```


Possible Causes

If the SCSI reserve/release feature is not enabled on your servers, data loss can be caused by configuration errors, incorrect paths, multiple master servers, incorrect SSO configurations and third-party or operating system utilities. If the SCSI reserve/release feature is enabled on all servers, then the cause could be third-party or operating system utilities running on the server that is also running the backup operation.

Unfortunately data loss cannot be prevented, just recognized after the fact. The NetBackup catalog is not cleaned up to remove information on prior backup sessions that were lost. The `bpexpdate` command must be run on the media id to clean up the catalog.

Disabling the Position Check

This check for data loss may be disabled by creating the following file on UNIX servers:

`/usr/openv/netbackup/db/config/NO_POSITION_CHECK`

This check for data loss may be disabled by creating the following file on Windows servers:

install_path`\netbackup\db\config\NO_POSITION_CHECK`

Checking for Tape/Driver Configuration Errors

On HP-UX, Solaris, AIX, TRU64, and Windows Servers

The `bptm` process detects data loss by reading the tape position and then checking the actual position against the expected position. Any configuration problem that causes the actual position to be greater than the expected position (at the end of the backup process), causes the following to occur:

- The tape is frozen.
- The backup fails.
- The following error message entry is placed in the error log:

  ```
  FREEZING media id xxxxxx, too many data blocks written, check
  tape/driver block size configuration
  ```

The backup data may be usable, in which case the image will need to be imported before restores can be done (using the `bpimport` command).

Possible Causes

The source of the configuration problem needs to be identified and corrected. The most common configuration error is the failure to configure the driver for variable length blocks.

A second source of the error could be in the tape driver's configuration data. On Solaris, this could be in `/kernel/drv/st.conf`. On IRIX, in the `/var/sysgen/master.d/scsi` file. Review the NetBackup Media Manager device configuration guide for the operating system you are using.

Disabling the Position Check

This check for data loss may be disabled by creating the following file on UNIX servers:

`/usr/openv/netbackup/db/config/NO_POSITION_CHECK`

This check for data loss may be disabled by creating the following file on Windows servers:

install_path`\netbackup\db\config\NO_POSITION_CHECK`

Issuing the Release

After a NetBackup process is done with the media, a SCSI release is issued as part of the unmount operation. This release frees the device for access by another HBA.

In addition, at the beginning of the startup process `avrd` issues a SCSI release to all configured tape devices that are currently in the Up state. This is done to release devices that were reserved at the time of a system re-boot or crash. The SCSI release command will return tape devices to general availability after a system crash.

Error Recovery

To recover a device that is reserved by an HBA that crashes or otherwise was unable to issue the SCSI release command, you can use the following option for the Media Manager `vmoprcmd` command:

`vmoprcmd -crawlreleasebyname` *drive_name*

This option requests all hosts that are registered to use the drive to release the drive (using the SCSI release command).

Issue the `vmoprcmd` command on the host that is the device allocator (DA host) or use the -h option on the command to specify the DA host.

Caution You can use this command after a PEND status has been displayed in **Device Monitor** in the NetBackup Administration Console, but do not issue this command during backups. See "Drive Status List of the Device Monitor" on page 65.

See your Media Manager system administrator's guide for the complete syntax and more information on using the `vmoprcmd` command.

SCSI Reserve/Release Logging and Conflict Notification

The `bptm` process logs all SCSI reserve/release commands. The `bptm` log should be checked on all hosts to ensure the SCSI reserve operation is being logged (look for SCSI RESERVE in the log).

The `avrd` process monitors all tape devices. NetBackup manages access to tape devices, such that a properly configured system will not receive the RESERVATION CONFLICT status from a tape device.

Reservation Conflict

If `avrd` gets a RESERVATION CONFLICT status, `avrd` changes the status of the device to PEND and writes the following message in the system log:

`Reservation Conflict status from` *DRIVENAME* `(device` *NUMBER*`)`

When the conflict is resolved, the following message will be written to the log:

`Reservation Conflict status cleared from` *DRIVENAME* `(device` *NUMBER*`)`

If this conflict occurs, some sort of mis-configuration is present (for example, the tape drive is reserved, but should not be) and the configuration problem should be corrected. A possible cause of this conflict is if an operating system crashes or a hardware failure has left a device reserved (see "Issuing the Release" on page 75).

Also in the **Device Monitor** or the output from the `vmoprcmd` command, PEND in the Control column means that a reservation conflict has occurred. See "Drive Status List of the Device Monitor" on page 65.

Operating System Limitations

HP-UX, TRU64, and Windows

These operating systems can not distinguish between a reserved device and a busy device. On these systems, PEND will also be reported if another application is using the device. This indicates a mis-configuration, as NetBackup cannot share tape devices with other applications. If you are using other applications, you should use the `tpreq` command or Down the drive before using the drive.

DYNIX, IRIX, and SVR4MP-RAS

These operating systems can not detect that a device is reserved. If the SSO scan host is running on one of these systems, no indication of this configuration problem will occur.

Issuing Reset Commands to Break a Reservation

On the following UNIX operating systems listed, you can try to reset a reservation conflict by using the associated reset commands.

Caution The reset operation may reset other devices in your configuration. Loss of data is also possible. Alternate methods of breaking the reservation on a device (using switch and bridge hardware) should be tried first.

Sun Solaris

Issue the following commands:

1. `mt -f` *drive_path_name* `forcereserve`
2. `mt -f` *drive_path_name* `release`

See the `mt(1)` man page for more information.

HP-UX

`st -f` *drive_path_name* `-r`

See the `st(1m)` man page for more information.

IBM AIX

`tctl -f` *drive_path_name* `reset`

See the `tctl` man page (in the IBM AIX Commands Reference) for more information.

SGI IRIX

Issue either of the following commands:

`scsiha -r` *bus_number*

`scsiha -L` *target_number bus_number*

See the `scsiha(1m)` man page for more information.

Controlling SCSI Reserve/Release

In the NetBackup 4.5 release using SCSI reserve for data integrity is on by default, but can be disabled by using an entry in the UNIX `bp.conf` file or in the registry on Windows servers.

The `bp.conf` file can be modified to contain a `DISABLE_SCSI_RESERVE` entry, which will turn off the use of SCSI reserve to all tape devices from this host.

The NetBackup UNIX and Windows GUIs have a checkbox to add or remove this entry in the bp.conf file or the registry. Select **NetBackup Management** > **Host Properties**. Select a master or media server in the right pane and then **Properties** > **Media > Disable SCSI Reserve**.

SCSI Reserve/Release Requirements and Limitations

The following topics cover important requirements and limitations.

Requirements

The following requirements are needed:

- There must be passthru driver access to all shared drives. The passthru driver must be installed and all required paths must be created.

  See the NetBackup Media Manager device configuration guide for information on configuring and using the passthru driver for various UNIX operating systems.

- Host operating systems must be set up properly to enable the SCSI reservation capability.

- Users of Sun Solaris 2.6 or 7 must install a ST driver patch to avoid a problem that keeps the device reserved when it should not be.

  For Solaris 2.6, the minimum patch level required is 105847-06. For Solaris 7, the minimum patch level required is 107460-06.

- Users of HP-UX must disable the operating system's use of SCSI reserve / release.

  See the topic, Enabling SCSI Reserve / Release in the HP 9000 chapter of the NetBackup Media Manager device configuration guide for instructions.

Limitations

This VERITAS implementation using SCSI reserve / release has the following limitations:

- NCR servers are unable to issue the SCSI reserve command and should be used with caution in a multi-initiator environment.
- SCSI reserve / release is not applicable for NDMP / FASTRAX configurations (no reserve command is available).
- Third-party copy configurations must be configured correctly. To retain reservation of a tape device when doing a third-party copy backup, refer to the description of the `mover.conf` file in the *NetBackup ServerFree Agent System Administrator's Guide for UNIX*.
- Cluster environments or multi-path environments with fail-over capability may leave devices reserved when fail-over occurs. If the fail-over does not break the device reservations, then the NetBackup use of SCSI reserve / release must be disabled.
- Cluster environments or multi-path environments with dynamic path sharing (TRU64 systems, for example) will cause backup and restore failures if the path changes. If path sharing cannot be eliminated, then the NetBackup use of SCSI reserve / release must be disabled.

Troubleshooting Tips 10

This chapter includes the following topics that may help you resolve SSO issues:

- SSO hardware guidelines.
- SSO software guidelines.
- A list of common problems.
- Frequently asked questions (FAQ).

SSO Hardware Guidelines

- Mixing SAN components can introduce problems. Always use a SAN configuration and firmware levels that are supported by the hardware vendors.
- Consult SAN device, HBA, and operating system documentation to determine how to configure operating system tape drivers and pass-thru drivers to detect your SAN devices.
- Check your hub timer settings.
- Using hard ALPA addresses, rather than soft addresses usually works the best. It is important to check with hardware suppliers to verify the recommended usage of their products.
- Check the firmware levels of all your fibre-channel hardware (for example, bridges) and make sure you are using the most recent level that is known to interoperate with other SAN hardware devices. Firmware levels change very rapidly.
- Try to duplicate SAN issues and problems using commands and utilities on the host operating system.
- Test backup and restore capabilities with dedicated tape drives before configuring them as shared drives.
- Test both backup and restore capabilities. It is possible to complete backups, but have unrecoverable images (for example, caused by incorrect switch settings).
- Ensure your hardware and SAN configuration is working and stable before adding SSO software.

- When building a large configuration, start drive sharing with a small number of tape drives and a small number (two or three) of media servers.
- Configuration and trouble shooting of SSO is much easier when done on a smaller scale. If possible, create multiple and independent SSO configurations with subsets of servers sharing subsets of SAN-attached drives.

Device Boot Order

Use the correct boot order for your fibre-channel hardware, as follows. Some smaller devices take a while to completely boot. Watch for any indicator lights to become green.

1. Robots or drives
2. Bridges
3. Hubs or switches (wait 3 or 4 minutes)
4. Hosts

SSO Software Guidelines

Media Manager Configuration Guidelines

Because of the great potential for creating incorrectly identified devices within an SSO configuration, it is recommended that you follow these practices:

- Use the Media Manager wizards to configure SSO. These wizards are available from the list of wizards displayed in the right pane of the **Media and Device Management** window of the NetBackup Administration Console.

  See “Why You Should Use the NetBackup Wizards” on page 35.

- If you are using the Device Configuration wizard, you should configure all shared drives from one host (this is usually the master server). Launch the wizard only once with the current host set to the master server. You then indicate a list of media servers (in the Device Hosts screen). The wizard will configure devices on all of the media servers you selected and these hosts will receive the shared configuration information.

  See “What To Expect In This Wizard” on page 39.

- Whether you have single or multiple masters, define only one host to contain the volume database.

If you are using the Device Configuration wizard on a new installation, the volume database host is set by default to be the master server (unless you did not accept the default settings during NetBackup installation).

- After configuring a subset of shared devices, use the configuration analyzer to check and point out any errors before continuing with other devices.

  See "Media and Device Management Configuration Analyzer" on page 67.

Operating System Guidelines

If errors occur during the installation and configuration of your SSO devices and you suspect the operating system, reference the following:

- Operating system logs, as described in the operating system documents.
- NetBackup logs.
- Operating system man pages (UNIX).
- The NetBackup Media Manager device configuration guide (UNIX).

Common Problems

- Using incompatible or outdated firmware or drivers in a hub, switch, HBA, or bridge.
- Using mismatched Gigabit Interface Converters (GBIC).
- Did not set JNI HBA failover value to zero seconds to avoid I/O hangs (bridge/HBA vendor fix).
- Using cluster configurations when they were not supported.
- Using vendor peripherals that only work on a fibre-channel arbitrated loop.
- Did not verify that SSO has been enabled on *each* server. You enable SSO using the Shared Drive license key. See "SSO Installation" on page 32.

  You can check keys by using the license key GUI available from the NetBackup **Help** menu on Windows servers or by using the `get_license_key` command on UNIX servers.
- Did not configure all of SSO from the master server. All configuration should be done from the master server, not from a media server.
- Did not configure the robotic path on every host. Remember that except for ACS and TLM robot types, only one host controls the robot.

- Did not select the appropriate device hosts when using the Device Configuration wizard, including the host with robotic control. See "What To Expect In This Wizard" on page 39.
- Created inconsistent configurations by using `tpconfig` to configure SSO rather using than the configuration wizards. These wizards have the added benefit of coordinating configurations across all hosts that are sharing the drives.
- Rebooted the host. Drives and robots that are connected by fibre channel cause increased complexity in a Media Manager device configuration. On some operating systems, the use of SCSI-to-fibre bridges may result in inconsistencies in the device paths when rebooting the host. After a reboot, the device configuration should be verified. Use HBA-to-driver binding when available.
- Using a drive name that is not consistent across all systems sharing drives.
- Did not test the drive paths on every media server.
- Did not define NetBackup storage units for each media server.
- (UNIX servers only)

  Did not use Berkeley-style close on the tape path.
- (On Sun Solaris servers only)

  Forgot to add tape configuration list entries in `/kernel/drv/st.conf`.

  Did not define configuration entries for expanded targets and LUNs in `sg.links` and `sg.conf` files.

  Problems in the entries in the `/etc/devlink.tab` file (created from `sg.links`). Check the following:

  - The first entry uses hexadecimal notation for the target and LUN. The second entry uses decimal notation for the target and LUN.
  - Use a single tab character between the entries, not a space or a space and a tab.

  Did not configure the operating system to forceload the `sg/st/fcaw` drivers.

  See the Sun chapter of the NetBackup Media Manager device configuration guide for more information.
- (On Tru64 or HP-UX servers only)

  Forgot to manually add device files.

FAQ

What combinations of SAN hardware components are supported for SSO?

SSO works with many hardware combinations. VERITAS has an open policy on hardware support for SSO. It is important to check with hardware suppliers to verify the interoperability of their products.

In an SSO configuration, I assume that once a server picks a tape drive and writes media, that media can only be written to again by that server. With existing NetBackup media servers today, a tape "belongs" to a media server until it expires or is deleted. Is this right?

Yes. Assigned media is still dedicated to a single server (see "SSO Restrictions and Limitations" on page 31). Be sure to define only one volume database host.

If I allocate four drives to a server and after an hour the server is finished with two of the drives and another server is requesting drives, will the two available drives be reallocated or does NetBackup wait until the backup schedule using the four drives is completely finished before reallocating the drives?

The two available drives will be reallocated and used. The NetBackup tape manager component is aware of drive status and notifies the NetBackup scheduler of drive availability.

Does the NetBackup SSO use IP protocol or SCSI protocol?

SSO uses IP protocol to pass control messages among peers.

Is it possible to set up drive cleaning for shared drives? I realize you can't use frequency-based cleaning, but can TapeAlert be used?

Yes. Using TapeAlert without frequency-based cleaning means that the tape will be cleaned only when the drive firmware (TapeAlert) requests a cleaning.

TapeAlert is not available for some types of drives, and some host platforms and adaptor connections. Since TapeAlert provides the same type of cleaning as library-based cleaning (robotic cleaning or auto cleaning), it is recommended that you disable library-based cleaning if using TapeAlert (for most vendor's robots).

SSO Reference Topics 11

This chapter includes the following topics:

- Supported SSO Components.
- SSO Components in Media Manager.
- Where to Go for More Information.

Supported SSO Components

Supported Robot Types

There is a distinction between Media Manager supported robot types and Media Manager supported robot types for SSO.

SSO is supported *only* for the following Media Manager robot types:

- ACS, TLH, and TLM (these are API robot types)
- TL8 and TLD

Media Manager robot types LMF, ODL, RSM, TL4, TS8, TSD, and TSH are *not* supported for SSO.

Supported Servers

The following table shows master server platform support for SSO:

Master Server	SSO Supported?
Sun Solaris	Yes
HP HP9000 HP-UX	Yes
IBM RS6000 AIX	Yes
Compaq Tru64 UNIX	Yes
Sequent DYNIX/ptx	Yes
SGI IRIX	Yes
Microsoft Windows NT (Intel only)	Yes
Microsoft Windows 2000 (Intel only)	Yes
NCR SVR4MP-RAS	No
Siemens Reliant UNIX	No
Linux	No

SSO Components in Media Manager

SSO utilizes the basic NetBackup and Media Manager processes and daemons to perform its tasks. `vmd` is the Media Manager volume daemon on UNIX hosts and the NetBackup Volume Manager service on Windows hosts. A major function of `vmd` is to manage media information. An additional function that `vmd` can provide is to be the device allocator (`DA`) for shared drives. In this case, `vmd` is known as `vmd/DA`.

vmd/DA

To coordinate network-wide allocation of tape drives, vmd/DA acts as a central clearing agent for all NetBackup and Storage Migrator shared tape requests in a storage area network. vmd/DA responds to requests from multiple instances of NetBackup Master Server, Media Server, or Storage Migrator (the versions of Media Manager must be the same).

For shared drive configurations, the host that is configured as the volume database host for a drive in a robot or a standalone drive is also known as the *device allocation host* (see "Device Allocation Host" on page 92). This is the host where vmd/DA resides. Other hosts in the configuration have vmd without device allocator functionality being utilized.

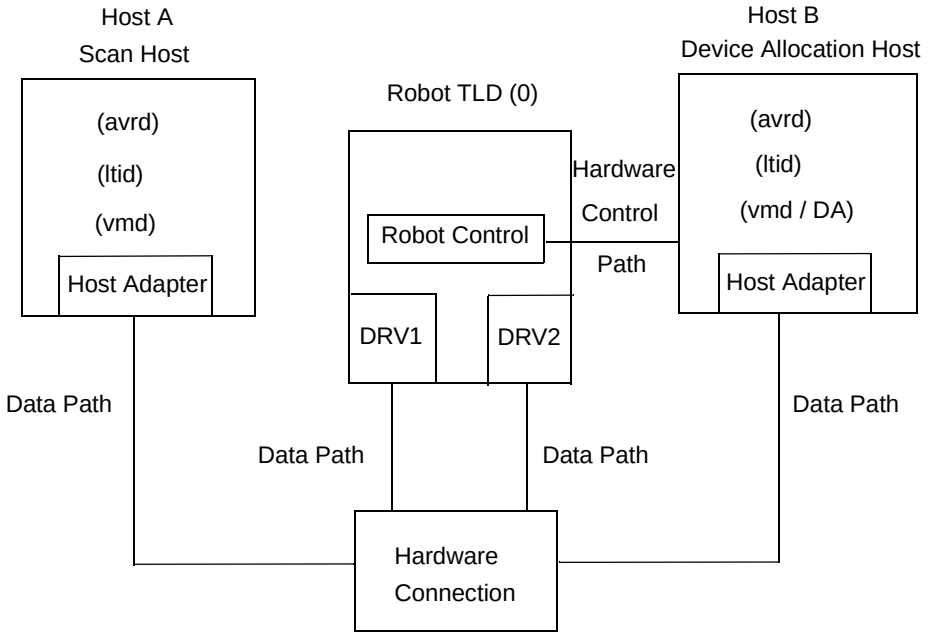
vmd/DA maintains shared drive and host information, such as a list of hosts that are registered to share a drive and which host currently has the drive reserved. Shared drive information is

- Modified by requests from ltid (the Media Manager device daemon on UNIX and the NetBackup Device Manager service on Windows).
- Dynamic, since it is built and maintained at runtime, rather than being stored on the device allocation host.

When ltid initializes on a device host, it calls vmd/DA with a list of shared drives. vmd/DA adds these drives and the host name to its configuration if necessary. Since ltid passes a complete list of drives each time, vmd/DA deletes references to drives for that host when a change in configuration removes them from that host's shared drive list. This deletion occurs when ltid is shut down gracefully or after it is restarted.

Sample SSO Configuration

The following figure shows an example of a shared drive configuration with Media Manager components.



In this figure, Host A is

- Connected to drives DRV1 and DRV2 through enabling hardware.
- The host where `ltid` was started first and called `vmd/DA` on the device allocation host (Host B) to register a shared drive. This action identifies Host A as the initial scan host (see "Scan Host" on page 91) for the drives.

In this figure, Host B

- Is connected to drives DRV1 and DRV2 through enabling hardware.
- Is configured to be the volume database host for the robot TLD (0) and therefore is also the device allocation host (see "Device Allocation Host" on page 92). `vmd/DA` is active on this host.
- Controls the robotics (except for ACS and TLM robot types, there is only one robot control host for each robot).
- Could be optionally configured as a Highly Available (HA) server.

Scan Host

Each shared drive has a host that is identified as the scan host. A *scan host* is the host where `avrd` (automatic volume recognition daemon / process) is scanning the drive when there is no other activity on that drive. A scan host must have data-path access to the drive.

Instances of `ltid` on hosts with the same shared drive configured, create `rdevmi` (remote device management interface) connections to the scan host to receive drive status information from the scan host. This information is used to maintain the shared drive information on the remote hosts.

How this Host is Determined

Scan hosts are determined by `vmd/DA` and may be different for each shared drive. The first device host that registers a shared drive with `vmd/DA` becomes the initial scan host for that drive.

All device hosts that register with `vmd/DA` pass a list of shared drives. The name of the currently assigned scan host for each drive is then returned to each registering host.

This Host Can Change

A scan host is assigned for a shared drive until some interruption occurs. For example, one of the following occurs:

- The socket connection, the host, the drive, or the network goes down.
- The drive is logically placed in the Down mode.

A new scan host is then chosen. If a scan host is declared unavailable, `vmd/DA` clears all reservations for that scan host and assigns a new scan host immediately, so that the requesting host can resume as soon as the previous scan host relinquishes its use of the drive.

The scan host temporarily changes to hosts that are requesting tape mounts while the mount is in progress. This happens so only one host at a time has access to the drive path.

A scan host for a drive needs to periodically re-register with `vmd/DA` to ensure that it remains the scan host. A host that is not identified as a scan host does not need to re-register until some disruptive event occurs (for example, a restart of `ltid` or a failure to get drive status data from the scan host for one or more drives).

Re-registering with `vmd/DA` keeps `vmd/DA` and the host that is registering in coordination with a dynamic shared drive configuration.

Device Allocation Host

The *device allocation host* is another name for the volume database host, when the volume database host performs tasks in support of SSO. This host is also the host where `vmd/DA` runs and manages the following:

- Reservations for shared drives on a host-by-host basis.
- A list of shared drives.
- A list of hosts that have registered to share a drive and where the drive is currently assigned.

How this Host is Determined

For SSO, the current volume database host for the drive is always the device allocation host for that drive.

If you follow the recommendations (see "Volume Database Host (Device Allocation Host)" on page 30) and configure one volume database host for a site, one device allocation host can manage multiple robotics connected to many media or master servers. These servers must be running the same version of Media Manager.

Where to Go for More Information

Configuring Shared Drives

For information on configuring shared drives using the Media Manager wizards, refer to the online product help in the wizards.

Configuring Fibre-channel on Solaris Platforms

Configuration information can be found in the Sun man pages on driver configuration or in the vendor's documentation.

Information on how to reconfigure the pass-thru driver can be found in the NetBackup Media Manager device configuration guide.

ACS Robots

See the ACS appendix in either of the following guides:

- *NetBackup DataCenter Media Manager System Administrator's Guide for UNIX*
- *NetBackup DataCenter Media Manager System Administrator's Guide for Windows*

TLH Robots

See the TLH appendix in either of the following guides:

- *NetBackup DataCenter Media Manager System Administrator's Guide for UNIX*
- *NetBackup DataCenter Media Manager System Administrator's Guide for Windows*

TLM Robots

See the TLM appendix in either of the following guides:

- *NetBackup DataCenter Media Manager System Administrator's Guide for UNIX*
- *NetBackup DataCenter Media Manager System Administrator's Guide for Windows*

Robot Slot Diagrams

See the Robot Drive and Slot Layout appendix in either of the following guides:

- *NetBackup DataCenter Media Manager System Administrator's Guide for UNIX*
- *NetBackup DataCenter Media Manager System Administrator's Guide for Windows*

Support Information for the Following:

- Operating Systems
- Devices and Firmware
- NetBackup DataCenter
- NetBackup Software Patches
- Windows Server Tape Drivers

Visit the VERITAS Support web site: `http://support.veritas.com`

Index